# 3. RUMÄNISCH-DEUTSCHE KONFERENZ ZUM EUROPÄISCHEN INFORMATIONSRECHT

Jürgen Taeger/Mihaela Drăgan/Sebastian Louven (Hrsg.)

# Aspekte des Informationstechnologierechts aus deutscher und rumänischer Perspektive

## Beiträge zur 3. Rumänisch-Deutschen Konferenz zum Europäischen Informationsrecht

OlWIR Oldenburger Verlag für Wirtschaft, Informatik und Recht

**Bibliografische Information Der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Gedruckt auf alterungsbeständigem säurefreiem Papier.

Alle Rechte vorbehalten.

© OlWIR Verlag

Oldenburger Verlag für Wirtschaft, Informatik und Recht
Rudolf-Kinau-Str. 54, 26188 Edewecht
mail@olwir.de

Edewecht 2020

ISBN: 978-3-95599-064-0

# INHALT

Jürgen Taeger / Mihaela Drăgan / Sebastian Louven
**Vorwort** ..... VII

Edgar Rose
**Videokameras im öffentlichen Raum – Fakten und Recht aus deutscher Sicht** ..... 1

Michaela Braun-Noviello
**Öffentliche Videoüberwachung aus der Perspektive des rumänischen Rechts** ..... 33

Jürgen Taeger
**Neue Entwicklungen im Beschäftigtendatenschutzrecht** ..... 43

Radu Hodis-Mayer
**Datenverarbeitung im Beschäftigungsverhältnis zur Aufdeckung von Straftaten** ..... 67

Gerd Kiparski
**The new european electronic communication code** ..... 75

Alexis Daj
**5G Network Economics: From Marketing Strategy to IoT and Blockchain Network Slicing Regulations** ..... 85

Irini Vassilaki
**Europäische Staatsanwaltschaft: Ein effektives Instrument zur Bekämpfung der Computerkriminalität?** ..... 105

Cristiana Fernbach/Cătălina Fînaru
**Blockchain legal trends** ..... 113

Gabriele Carovano
**The Digitalisation of the economy and the needed reform of the ECN** ..... 127

# VORWORT

Die Babeş-Bolyai-Universität Cluj-Napoca war wieder Gastgeberin der nunmehr 3. Rumänisch-Deutschen Konferenz zum Europäischen Informationsrecht. Erneut trugen Juristinnen und Juristen aus der Wissenschaft, aus der Anwaltschaft, aus internationalen Institutionen und aus Unternehmen zu aktuellen Fragen des Informationstechnologierechts vornehmlich aus der Perspektive ihres Mitgliedstaates vor. Die Diskussion der Teilnehmerinnen und Teilnehmer aus Rumänien, Deutschland, Griechenland, Italien und Ungarn war lebhaft und sehr konstruktiv.

Ein Teil der Vorträge dieser wichtigen grenzüberschreitenden wissenschaftlichen Veranstaltung werden in diesem Tagungsband dokumentiert. Die Herausgeber bedanken sich bei allen Teilnehmern für ihr Engagement und freuen sich auf die 4. Rumänisch-Deutsche Konferenz zum Europäischen Informationsrecht vom 29.-30. Mai 2020 in Cluj-Napoca (Klausenburg).

Oldenburg/Cluj Napoca, im Dezember 2019

**Prof. Dr. Prof. h.c. Jürgen Taeger**

Carl von Ossietzky Universität Oldenburg
Direktor des Interdisziplinären Zentrums
für Recht der Informationsgesellschaft (ZRI)
Vorsitzender der Deutschen Stiftung
für Recht und Informatik (DSRI)

**Prof. Dr. Mihaela Drăgan**

Babeş-Bolyai-Universität Cluj-Napoca
Vizedekanin, Fakultät für Wirtschaftswissenschaften
und Unternehmensführung

**Ass. iur. Sebastian Louven**

Carl von Ossietzky Universität Oldenburg
Interdisziplinäres Zentrum für Recht
der Informationsgesellschaft (ZRI)

# VIDEOKAMERAS IM ÖFFENTLICHEN RAUM – FAKTEN UND RECHT AUS DEUTSCHER SICHT

Edgar Rose

Interdisziplinäres Zentrum für Recht der Informationsgesellschaft (ZRI),
Carl von Ossietzky Universität Oldenburg
edgar.rose@uol.de

## Zusammenfassung

Etwa 60-80 % der deutschen Bevölkerung begrüßen die Videoüberwachung insbesondere durch Polizei und Behörden, da sie sich dadurch mehr Sicherheit im öffentlichen Raum erhoffen (1.). Dass die erwünschten Wirkungen tatsächlich eintreten, wird in Untersuchungen nur zum Teil bestätigt. Unzureichend untersucht sind zudem unerwünschte Wirkungen, die durch die weiträumige Videoerfassung unzähliger Passanten entstehen (2.). Die deutsche Rechtsprechung aus Zeiten vor Anwendung der Datenschutzgrundverordnung auf Grundlage von § 6b BDSG a.F. konnte der rasanten Ausbreitung der Videoüberwachung wenig entgegensetzen (3.). Seit 2018 ist allerdings ein verschärfter Prüfungsmaßstab auf höchstrichterlicher Ebene zu beobachten. Obwohl sich die Anforderungen, die sich aus der DSGVO an die Zulässigkeit von Videoüberwachungsmaßnahmen ergeben, nicht wesentlich vom hergebrachten nationalen Recht unterscheiden (4.), hat sich die Sensibilität für den Datenschutz nicht nur in der Fachdebatte, sondern auch in der aktuellen Rechtsprechung zur Videoüberwachung erhöht (5.). Dennoch ist zweifelhaft, ob dies allein genügt, um die Videoüberwachung im öffentlichen Raum auf ein sinnvolles und sozialverträgliches Maß zu begrenzen. Weitere Maßnahmen technischer Regulierung sind in Betracht zu ziehen (6.).

## 1 Einstellungen zur Videoüberwachung in Deutschland

Die Installation von Videoüberwachungsanlagen im öffentlichen Raum ist in Deutschland ein oft sehr umstrittenes Thema. Die gegenläufigen Anliegen, einerseits Sicherheit in der Öffentlichkeit gegenüber Straftaten zu erhöhen und andererseits Privatsphäre sowie persönliche Daten auch in der Öffentlichkeit zu schützen, befeuern scharfe Kontroversen. Das gilt vor allem für alle Anlässe des weiteren Ausbaus einer ohnehin schon engmaschigen Videoüberwachung. Umstritten ist, in welchem Ausmaß und – angesichts intelligenter Technologien – in welcher technischen Ausstattung dies geschehen soll.[1] Dabei gilt es jedoch zu unterscheiden. In den staatlichen Institutionen sowohl des politischen Systems als auch des Rechtssystems

[1] Siehe etwa die Antwort der Bundesregierung auf die kleine Anfrage der Fraktion DIE LINKE im Deutschen Bundestag vom 23.8.2018, BT-Drs. 19/3931.

wird der Streit wesentlich heftiger ausgetragen als in der Bevölkerung allgemein.

### 1.1 Staatliche Sichtweisen

Unbestritten gilt, dass Sicherheit im öffentlichen Raum ein Grundanliegen in einer zivilisierten Gesellschaft ist. Das öffentliche Leben sollte sich frei von Bedrohung und Angst entfalten können.[2] Hierzu kann ein Ausbau der Videoüberwachung nach Auffassung der Befürworter – u.a. der Bundesregierung[3] – einen wichtigen Beitrag leisten, indem sie von Straftaten gegen Leib und Leben abschreckt oder jedenfalls die Verfolgung der Täter unterstützt.

Videoüberwachung erfasst allerding alle Personen, die sich im öffentlichen Raum aufhalten, und beeinflusst deren Lebensgefühl und Verhalten. Ende 2018 hat das Bundesverfassungsgericht unterstrichen, dass es zur Freiheitlichkeit eines Gemeinwesens gehöre, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen könnten, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein.[4] Dass dies nicht nur für staatliche Überwachungsmaßnahmen gelten sollte, betont der „Düsseldorfer Kreis“ der unabhängigen Datenschutzbehörden in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“. Jeder Mensch, heißt es, habe grundsätzlich das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mit Hilfe von Kameras beobachtet oder aufgezeichnet wird.[5]

Dass dieses Recht aktuell in den Ortszentren massiv in Frage gestellt wird, ist durch die intensivierte Kennzeichnungspraxis als Folge der DSGVO seit 2018 noch augenfälliger geworden. Massenhaft springen die Hinweisschilder zu privaten Überwachungsanlagen nunmehr ins Auge. Zu den vielen festinstallierten kommen noch zahlreiche mobile Kameras vor allem in Fahrzeugen, an Drohnen oder am Körper getragen, auf die meistens[6] keinerlei Hinweise gegeben werden.[7]

---

[2] Zur Einschüchterung der öffentlichen Debatte im Netz durch Hasskommentare siehe die repräsentative Untersuchung von *Geschke/Klaßen/Quent/Richter*, #Hass im Netz: Der schleichende Angriff auf unsere Demokratie, S. 28 f.

[3] BT-Drs. 18/10941, S. 8; BT-Drs. 19/3931, S. 2.

[4] Entscheidung zur staatlichen automatisierten Kraftfahrzeugkennzeichenkontrolle in Bayern, BVerfG, Beschl. v. 18.12.2018 – 1 BvR 142/15, NVwZ 2019, 381, Rn. 51.

[5] *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, S. 3.

[6] Mit Ausnahme der Bodycams von Polizei und anderen Einsatzkräften.

[7] Siehe die Beiträge in *Taeger*, Chancen und Risiken von Smart Cams im öffentlichen Raum.

## 1.2 Einstellungen in der Bevölkerung

Vergleichsweise gut erforscht ist die Akzeptanz der Videoüberwachung in der deutschen Bevölkerung. *Kudlacek* beschreibt 10 vorhandene Studien, bevor er auf selbst im Jahre 2010 erhobene Daten eingeht.[8] Basierend auf 1398 Befragungen von Fluggästen am Flughafen Hannover kommt er u.a. zu dem Ergebnis, dass 53,1 % der Aussage zustimmen, dass Videoüberwachung zur Sicherheit der Bürger zunehmend eingesetzt werden sollte. 21,8 % lehnen dies ab.[9] Ein ähnlicher Ablehnungswert von ca. 20 % war auch schon 2005 aus Brandenburg berichtet worden, während in den verschiedenen Orten 66-86 % die eingeführte Videoüberwachung positiv bewerteten.[10]

Besonders interessant sind die Befragungsbefunde zur Frage eines erhöhten Sicherheitsgefühls. Rund 55,5 % der Befragten fühlten sich nach der Studie aus Brandenburg durch die Videoüberwachung sicherer und hatten weniger Angst, 40,5 % der Befragten gaben an, dass die Videoüberwachung keine konkreten Auswirkungen auf ihr Sicherheitsempfinden hatte.[11] Zu ähnlichen Werten kommt eine Forsa-Studie 2018, wonach 53 % der Befragten den Einsatz von Videoüberwachung für das persönliche Sicherheitsempfinden als „sehr wichtig“ oder „wichtig einstuften“, währen 47 % angaben, dass die Videoüberwachung für ihr Sicherheitsempfinden „weniger wichtig“ oder „unwichtig“ sei.[12] Gute Beleuchtung bei Nacht und hohe Polizeipräsenz finden danach wesentlich höhere Zustimmung bei der Frage nach dem Sicherheitsempfinden.

Dass die Zahl derer, die ein erhöhtes Sicherheitsempfinden angeben, deutlich kleiner ist als die Zahl der Befürworter der Videoüberwachung, könnte damit zusammenhängen, dass viele Befragte die begrenzte Wirksamkeit der Kameras (siehe 2.1) realistisch einschätzen können.

---

8 *Kudlacek,* Akzeptanz von Videoüberwachung, S. 44 ff.

9 Ebenda, S. 111.

10 *Bornewasser*, Evaluation der polizeilichen Videoüberwachung öffentlicher Straßen und Plätze im Land Brandenburg, S. 118 ff.

11 Ebenda.

12 *Forsa Politik- und Sozialforschung GmbH*, Sicherheit in der Stadt - Ergebnisse einer repräsentativen Bevölkerungsbefragung, S. 11.

# 2 Faktische Wirkungen der Videoüberwachung

Bevor auf erwünschte und unerwünschte Wirkungen der Videoüberwachung eingegangen wird, sei ein kurzer Blick auf den Bestand an Videoüberwachungsanlagen in Deutschland geworfen.[13] Gesicherte Zahlen existieren nicht, da es eine Meldepflicht nicht gibt. Vielfach werden daher von privater Seite Geräte im Internet, Bau- oder Elektronikmarkt erworben, am bzw. im eigenen Gebäude installiert und dann abgewartet, ob sich erfasste Personen dagegen zur Wehr setzen. Gelegentlich geschieht dies durchaus, vor allem durch eine Beschwerde bei der Datenschutzbehörde.

Etwas besser ist bekannt, wie viele Kameras von öffentlicher Seite (Polizei, Kommunen, ÖPNV) eingesetzt werden. Für Köln hat der Stadt-Anzeiger 2018 knapp 4000 Kameras recherchiert.[14] Für München waren es schon 2015 knapp 10 000 Kameras öffentlicher Betreiber.[15] Die Bundesregierung hat für deutsche Bahnhöfe 2018 insgesamt 6000 Kameras angegeben.[16] Überall steht ein weiterer Ausbau im Raum. Neue technische Entwicklungen zur automatischen Erkennung der Identität oder gefährlicher Situationen sind in der Erprobungsphase.[17]

## 2.1 Erwünschte Wirkungen auf die Sicherheit im öffentlichen Raum

Die Verwirklichung erhöhter Sicherheit im öffentlichen Raum durch Videoüberwachung könnte insbesondere an der Abnahme von Straftaten im überwachten Bereich oder an Fällen erleichterter Aufklärung von Straftaten abgelesen werden. Eine große Anzahl von empirischen Studien, die vor allem in den USA und im Vereinigten Königreich durchgeführt worden sind, hat sich bereits mit der Frage befasst, inwieweit Kriminalität durch Videoüberwachung zu beeinflussen ist. Eine 2018 zum zweiten Mal erweiterte Meta-Studie von *Piza/Welsh/Farrington/Thomas*, die nunmehr 76 Einzelstudien zusammenfasst, kommt zu dem Ergebnis, dass Kriminalität durch den Einsatz von Videoüberwachung durchschnittlich um 13 % sinkt, wenn man

---

[13] Statistisch erfasst sind nur Teilbereiche des Videoeinsatzes öffentlicher Stellen und der Deutschen Bahn, vgl. *Scholz,* in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, Art. 6 DSGVO Anh. 1 Rn. 5 Fn. 15.

[14] www.ksta.de/koeln/ueberwachte-stadt-koelner-werden-mit-mehr-als-4000-kameras-fast-dauerhaft-gefilmt-30424870.

[15] www.sueddeutsche.de/muenchen/videoueberwachung-in-muenchen-stadt-der-10-000-augen-1.2316618.

[16] BT-Drs. 19/3931, S. 2.

[17] SWR, 4.7.2019: Intelligente Videoüberwachung in Mannheim bald im Realbetrieb, www.swr.de/swraktuell/baden-wuerttemberg/mannheim/Videoueberwachung-in-Mannheim,videoueberwachung-mannheim-bilanz-104.html, vgl. zur Rechtslage *Desoi*, Intelligente Videoüberwachung.

die Entwicklung in überwachten und nicht-überwachten Gebieten vergleicht.[18] Eine andere Meta-Studie, die mit einer speziellen Methodik auf insgesamt nur sieben Erhebungen vertraut, kommt zu dem deutlich optimistischeren Ergebnis, das der Rückgang der Kriminalität zwischen 24 und 28 % beträgt.[19]

Deutsche Studien sind deutlich weniger zahlreich und lassen wissenschaftliche Begleitforschung oft vermissen.[20] Das ist bedauerlich, da landestypische bzw. kulturelle Unterschiede die Wirkung durchaus beeinflussen, wie der Vergleich zwischen Ergebnissen aus den USA und dem Vereinigten Königreich zeigt.[21] Eine der wissenschaftlich fundierten Studien zu innerstädtischen Kriminalitätsschwerpunkten im Jahre 2005 in Städten Brandenburgs ergab ungewöhnlich heftige Ausschläge in der Kriminalitätsstatistik. In drei Orten sank die Kriminalität im videobeobachteten Bereich um 30-60 %, in einem vierten Ort stieg sie hingegen um 30 %.[22] Ganz im Gegensatz dazu stehen Studien, in denen die Einführung der Videoüberwachung keinerlei Wirkung auf Kriminalitätsraten zu haben schien.[23]

Eine aktuelle kriminologisch fundierte Studie aus Deutschland bezieht sich auf die Städte Aachen, Dortmund, Duisburg, Düsseldorf, Essen und Köln, in denen Ende 2016 bzw. 2017 Videoüberwachungsanlagen an Brennpunkten des Kriminalitätsgeschehens des jeweiligen Stadtgebietes installiert worden sind.[24] Die Ergebnisse sind auch hier sehr uneinheitlich. Eine verstärkt rückläufige Kriminalität im überwachten Bereich verglichen zum gesamten Stadtgebiet, in dem die Kriminalität zeitgleich ebenfalls rückläufig war, kann diese Studie nur für vier der sechs Städte feststellen. In Aachen sinkt die einschlägige Kriminalität im gesamten Stadtgebiet stärker als im überwachten Bereich. In Dortmund steigt sie im überwachten Bereich sogar, während sie insgesamt im Stadtgebiet sinkt. Dagegen ergibt

---

[18] *Piza/Welsh/Farrington/Thomas*, CCTV and Crime Prevention, S. 18.

[19] *Alexandrie*, Journal of Scandinavian Studies in Criminology and Crime Prevention 18, S. 210.

[20] Siehe die Auswertung von *Brandt*, Wirkungen situativer Kriminalprävention.

[21] *Piza/Welsh/Farrington/Thomas*, CCTV and Crime Prevention, S. 29.

[22] Bericht der Landesregierung an den Landtag über die polizeiliche Videoüberwachung öffentlich zugänglicher Straßen und Plätze zu präventiven Zwecken im Land Brandenburg, Landtag Brandenburg – Drucksache 4/2347, 4.1.2006, S. 4-17.

[23] So *Hempel/Alisch*, Evaluation der 24-Stunden-Videoaufzeichnung in U-Bahnstationen der Berliner Verkehrsbetriebe (BVG) – Zwischenbericht; keine Auswirkung auch in Luzern laut *Zehnder*, Kameraüberwachung als Präventionsinstrument im öffentlichen urbanen Raum für den Bahnhofplatz der Stadt Luzern.

[24] *Glaubitz/Kudlacek/Neumann/Fleischer/Bliesener*, Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen.

sich in Duisburg und Essen ein deutlich verstärktes Absinken der Kriminalität in den Gebieten unter Videoüberwachung. Aggregiert ergibt diese Studie ein durchschnittlich um knapp 5 % verstärktes Absinken der Kriminalität durch Videoüberwachung.[25] Auch hinsichtlich der Aufklärungsquote zeigt diese Studie positive Auswirkungen. Sie stieg nach Einführung der Videoüberwachung durchschnittlich um 5,7 % im überwachten Bereich gegenüber einem Anstieg von nur 1,6 % in den gesamten Stadtgebieten.[26]

Fazit: Alle vorhandenen Studien und Meta-Studien machen eines klar. Videoüberwachung führt nicht zu kriminalitätsfreien Räumen. Es geht immer nur um eine mögliche Reduzierung von Kriminalität. Unter günstigen, aber noch ungeklärten Umständen ist lokal ein Absinken um bis zu 60 % durch Videoüberwachung möglich. So wurden etwa in Duisburg die Zahlen für schweren und einfachen Diebstahl halbiert.[27] An anderer Stelle dagegen scheint der Effekt völlig auszubleiben. Durchschnittswerte liegen zwischen 5 und 15 % Absinken der gesamten Straßenkriminalität durch Einsatz von Videokameras. Vermutet wird, dass die Art der Implementierung der Videoüberwachung Auswirkungen auf den Erfolg hat.[28] Die Intensität der Kenntlichmachung und die sonstige Publizität dürften z.B. den Abschreckungseffekt beeinflussen.

Es gibt also entgegen Auffassungen in der Rechtsprechung[29] keinen allgemeinen Erfahrungssatz, dass Videoüberwachung abschreckend im Hinblick auf kriminelle Aktivitäten tatsächlich wirkt. Es ist sogar möglich, dass eine schlecht implementierte Videoüberwachung gar nicht wirkt oder paradoxe Effekte hat, z.B. weil sie die Beteiligten in falscher Sicherheit wiegt. Ob eine Maßnahme zur Kriminalitätsbekämpfung geeignet ist, muss also in jedem Einzelfall anhand von Tatsachen beurteilt werden.

### 2.2 Unerwünschte Wirkungen auf erfasste Passanten

Im Frühjahr 2016 fand das Projekt eines russischen Fotografen unter Anwendung der Gesichtserkennungssoftware FindFace allgemeine Aufmerksamkeit. Der Slogan „Your face is big data“ beschrieb das Ergebnis, dass bei rund 70 % der zufällig in der U-Bahn fotografierten Personen allein das Bild mit Hilfe des Internets zunächst die Identität sowie im Anschluss zahlreiche persönliche Zusatzinformationen aus dem Netz offenbart.[30] Darüber

[25] Ebenda, S. 38 f.

[26] Ebenda, S. 49.

[27] Ebenda, S. 88.

[28] Ebenda, S. 57.

[29] Vgl. OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, BeckRS 2017, 137554, Rn. 37.

[30] *Kühl*, Superfood für Algorithmen, Zeit Online, 4.5.2016.

hinaus kann dem fotografierten Gesicht eines Menschen weit mehr als die Identität entnommen werden. Big Data ist unmittelbar im Bild enthalten, indem sich psychische und physische Zustände vor allem aus der Mimik der Gesichtsmuskulatur erschließen lassen.[31] Auch an dem Versuch, Charaktereigenschaften aus dem Gesicht unter Anwendung künstlicher Intelligenz zu lesen, wird gearbeitet. Der Anbieter „Faception" ist mit einer Gesichts-Persönlichkeitsanalyse bereits auf dem Markt,[32] auch wenn das Thema wissenschaftlich äußerst umstritten ist.[33]

Bei der Analyse der unerwünschten Wirkungen der Videoüberwachung sind zwei sehr unterschiedliche Aspekte zu unterscheiden. Videokameras können die Rechte der bildlich Erfassten einerseits durch „Informationelle Fremdbestimmung" und andererseits durch „Beobachtungsdruck" beeinträchtigen.

### 2.2.1 Informationelle Fremdbestimmung

Bilder wecken Aufmerksamkeit, sprechen Emotionen spontan an, werden blitzschnell aufgenommen und graben sich tief in das Gedächtnis ein. Sie sind Texten in diesen Punkten weit überlegen, wie vielfältige Studien belegen.[34] Man spricht daher von der besonderen „Macht der Bilder".[35] Das Herstellen und die Verwendung von Bildern, die Personen zeigen, können ungleich tiefer in deren Selbstbestimmungsrechte eingreifen als die Verwendung sonstiger personenbezogener Daten, die begrifflich oder in Zahlenwerten schriftlich festgehalten werden. Ein zentraler Grund dürfte in der hohen und zugleich schwer kalkulierbaren Informationsfülle liegen, die das Bild eines Menschen und insbesondere seines Gesichts dem Betrachter übermittelt. Die Videoüberwachung liefert im Unterschied zum Foto dazu auch noch bewegte Bilder und damit zusätzliche Informationen etwa zum Gangbild, das ebenfalls physische und psychische Zustände spiegeln kann.

Besonders Gesichter ziehen das Interesse jedweder Bildbetrachter auf sich. In einer Zehntelsekunde werden nicht nur Alter, Geschlecht und emotionaler Zustand, sondern auch zentrale Charaktereigenschaften (z.B. Ver-

---

[31] Zum aktuellen Stand der Emotionsanalyse anhand von Gesichtsbildern *Reinhold/Wortmann*, Von der Gesichtsdetektion zur Emotionsanalyse, Marketing Review St. Gallen, S. 888 (891 f.).

[32] *Lobe*, Zeig mir dein Gesicht, Frankfurter Allgemeine, 28.5.2016.

[33] Kritisch *Todorov*, Can we read a person's character from facial images?, Scientific American, 14.5.2018.

[34] Vgl. den Forschungsüberblick bei *Lobinger*, Visuelle Kommunikationsforschung, S. 76 ff.

[35] Ausführlich *Boehme-Neßler*, BilderRecht, S. 55 ff.; *Lobinger*, Visuelle Kommunikationsforschung, S. 87.

trauenswürdigkeit, Kompetenz) sowie die Einstellung zu dieser Person (attraktiv, sympathisch) eingeschätzt.[36] Die meisten Menschen wissen um die „Macht des ersten Eindrucks", auch wenn die einzelnen Aspekte des Vorgangs keineswegs durchschaut werden. Um diesen dennoch zu steuern, kleiden sie sich gezielt, richten die Haare oder schminken sich. Soll ein Foto gemacht werden, wird eine spezielle Pose (Körperhaltung, Gesichtsausdruck) eingenommen. Umso verhasster ist es vielen, spontan oder gar unbemerkt aufgenommen zu werden, vor allem wenn dies durch Fremde geschieht. Denn das so entstandene Bild ist dem eigenen Einfluss entzogen. Seine Verwendung liefert möglicherweise Informationen oder auch Fehlinformationen, die den eigenen Selbstdarstellungswünschen widersprechen. Fortschreitende Bildanalysemöglichkeiten künstlicher Intelligenz werden das Problem weiter verschärfen, wenn sie die ungeschminkte Realität ans Licht fördern oder gar fälschlich den Eindruck erwecken, dass sie das könnten.

Zukünftig werden Personen auf den Videobildern zunehmend zuverlässig automatisch erkannt werden, womit die Möglichkeit entsteht, die Bilder unterschiedlicher Aufnahmegeräte zur gleichen Person automatisch zusammenzuführen und damit die Aussagekraft weiter zu erhöhen. Dass die Bilddaten aus den verschiedenen Videokameras unterschiedlicher privater Verwender tatsächlich für eine solche Zuordnung zusammenfließen, ist durchaus denkbar. Grundsätzlich gilt, dass alle Videoüberwachungsgeräte, die ans Internet angeschlossen sind, gehackt werden können.[37] Geräte mit entsprechenden Sicherheitslücken sind auch schon identifiziert worden.[38] Auch gibt es im Netz Anbieter, deren Dienstleistung genau darin besteht, das Videomaterial unterschiedlicher Verwender zu speichern und auszuwerten, das ihnen zu diesem Zweck übermittelt wird (Video Surveillance as a Service - VSaaS).[39] Entgegen OVG Saarlouis[40] ist also die Gefahr einer unkontrollierten Weitergabe sehr real.

### 2.2.2 Erhöhter Beobachtungsdruck

Der besondere Eingriff in die Persönlichkeitsrechte der Betroffenen erfolgt auch schon im Vorfeld tatsächlich aufgenommener Bilder. Wenn die reine Möglichkeit, abgebildet zu werden, antizipiert wird, entsteht auch so be-

---

[36] *Willis/Todorov*, Psychol. Sci. 2006, S. 592 ff.

[37] *Hurtz*, Kriminelle könnten Millionen Überwachungskameras übernehmen, SZ.de, 10.10. 2018.

[38] Ebenda.

[39] https://memoori.com/ai-cloud-services-making-intelligent-video-surveillance-increasingly-smart-affordable/.

[40] OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, BeckRS 2017, 137554, Rn. 40.

reits Beobachtungsdruck. Der Weg durch die Fußgängerzone kann zur permanenten Pose werden, weil Fotoaufnahmen aus allen Richtungen drohen. Spätestens wenn Kameras zu sehen sind, werden vielfach jene psychischen Abläufe ausgelöst, die unter Beobachtung typisch sind. Dazu gehört vor allem ein gesteigerter Zustand der Selbstaufmerksamkeit („self-awareness"),[41] in dem die Person überprüft, ob sie sich gerade so wie beabsichtigt präsentiert. Beobachtung führt demnach typischerweise zu Selbstbeobachtung.

Hingewiesen wird in der Fachliteratur häufig darauf,[42] dass dies nicht nur eine gravierende persönliche Beeinträchtigung darstellt, sondern in letzter Konsequenz auch das gesellschaftliche bzw. politische Leben durch Anpassungsdruck verarmt. Schon den „Erfindern" des „Rights to Privacy" Warren und Brandeis ging es 1890 u.a. um den Schutz eines sonst schwindenden Individualismus.[43] Der entscheidende Punkt ist, dass nach der Theorie objektiver Selbstaufmerksamkeit Menschen im Zustand gesteigerter Selbstaufmerksamkeit ihr Selbst hinsichtlich Verhalten, Charakterzüge oder Einstellungen mit Standards korrekten Verhaltens, korrekter Charakterzüge oder korrekter Einstellungen automatisch abgleichen.[44] Wird bei diesem Abgleich eine Diskrepanz festgestellt, so die Theorie, wird dies als unangenehm empfunden. Die Person reagiert mit dem Wunsch, das Selbst mit den Standards in Einklang zu bringen. Im allgemeinen dürften daher Bemühungen einsetzen, das abweichende Verhalten usw. an die Standards anzupassen, da sich Verhalten in der Regel leichter ändern lässt als Verhaltensstandards. Diese Reaktion ist in vielen Experimenten nachgewiesen.[45] Unter bestimmten Umständen allerdings werden auch die Standards in Frage gestellt und Menschen verhalten sich gezielt abweichend. Einzelheiten sind weitgehend unerforscht.

### 2.3 Ergebnis

Hinsichtlich der Wirksamkeit von Videoüberwachung im öffentlichen Raum ist nur gesichert, dass ein hoher Anteil der Bevölkerung sie befür-

[41] Das Erklärungskonzept stammt aus den 1970er Jahren und ist seither durch zahlreiche Studien belegt worden. Grundlegend: *Duval/Wicklund*, A theory of objective self-awareness; *Carver/Scheier*, Attention and self-regulation: a control-theory approach to human behavior, S. 143 ff.

[42] Eingehend *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, S. 35 ff.; *Schwenke*, Private Nutzung von Smartglasses im öffentlichen Raum, S. 80 ff.

[43] *Glancy*, The Invention of the Right to Privacy, Arizona Law Rev. 1979, S. 1 (22 f.).

[44] *Silvia/Duval*, Objective Self-Awareness Theory: Recent Progress and Enduring Problems, Personality and Social Psychology Review 5, S. 230 (231).

[45] Ebenda, S. 233.

wortet und immerhin noch eine Mehrheit sie als wichtig für ihr persönliches Sicherheitsempfinden einstuft. Ob Videoüberwachungsanlagen tatsächlich die Sicherheit erhöhen, kann hingegen nicht generell bestätigt werden. Gleiche Untersuchungen in verschiedenen Städten kommen zu gegensätzlichen Ergebnissen. Es scheint also stark von den Umständen des Einzelfalls abzuhängen, ob Videoüberwachung im Sinne von Prävention und Repression tatsächlich wirkt.

Videoüberwachung wirkt nicht nur auf potenzielle Straftäter, sondern auch auf Bürgerinnen und Bürger, die nichts Böses beabsichtigen. Der sogenannte Beobachtungsdruck führt zu erhöhter Selbstaufmerksamkeit, die das Individuum unter Stress setzt und vielfach zu Anpassungsreaktionen motiviert. Hinzu kommt der mögliche Missbrauch der Bilddaten bzw. der auf Grundlage der Bilder analytisch ermittelten personenbezogenen Daten ohne Wissen und Wollen der Betroffenen.

## 3 Erforderlichkeit und Interessengerechtigkeit der Videoüberwachung in der Rechtsprechung

Im BMBF-geförderten Forschungsprojekt „Chancen und Risiken von Smart Cams im öffentlichen Raum“ sind mehrere Urteile hoher Gerichte aus der letzten Phase vor Geltung der DSGVO analysiert worden. Ziel war es, besser zu verstehen, warum die Verbreitung auch privater Videoüberwachung trotz der genannten Risiken rasch zunehmen konnte, ohne dass dem die Rechtsprechung spürbar entgegengetreten wäre.

Ausgewählt wurden daher gezielt drei Urteile aus den Jahren 2017/18 mit der einheitlichen Tendenz, überwachungskritische Entscheidungen der Behörden und unterer Instanzen aufzuheben. Am spektakulärsten ist insoweit die Dashcam-Entscheidung des BGH,[46] in die gleiche Richtung gehen die Apotheken-Überwachungsentscheidung des OVG Saarlouis[47] und die Entscheidung des OVG Lüneburg[48] zur Videoüberwachung im öffentlichen Nahverkehr. Es gibt aus dieser Zeit auch Urteile, die das Behördenhandeln gegen Formen der Videoüberwachung (teilweise) bestätigen.[49] Aber die drei genannten Entscheidungen eignen sich besonders, wissenschaftlich zu

[46] BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883.

[47] OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, ZD 2018, 134.

[48] OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, ZD 2018, 50.

[49] OVG Berlin-Brandenburg, Urt. v. 6.4.2017 – OVG 12 B 7.16, ZD 2017, 399; OLG Celle, Beschl. v. 4.10.2017 – Ss (OWi) 163/17, RDV 2018, 29.

untersuchen, woran genau in der gerichtlichen Überprüfung der Privatsphärenschutz bei der Videoüberwachung scheitern kann. Die Analysen des Forschungsprojekts werden hier veröffentlicht.

### 3.1 Videoüberwachung im ÖPNV (OVG Lüneburg)

Die ÜSTRA Hannoversche Verkehrsbetriebe AG setzt in Bussen und Bahnen feststehende Videokameras ein, mit denen durchgehend Bilder vom Fahrzeuginnenraum aufgezeichnet werden. Der Speicher befindet sich fest in den Fahrzeugen verbaut und wird als Ringspeicher nach 24 Stunden überschrieben. Nach dem Blackbox-Verfahren findet eine Überwachung in Echtzeit nicht statt. Nur bei Anlass zur Auswertung der Aufzeichnungen werden diese gesichert. Gegen den Bescheid des Landesbeauftragten für den Datenschutz Niedersachsen vom 29. August 2014, die Videoüberwachung während des Einsatzes der Fahrzeuge im ÖPNV einzustellen, klagte die ÜSTRA und bekam beim VG Hannover zunächst aus formalen Gründen Recht.[50] Die Behörde wollte aber per Rechtsmittel beim OVG weiterhin einen differenzierten Einsatz von Videokameras je nach Zeitpunkt und Linie unter Berücksichtigung der jeweils konkreten Gefahrenlage durchsetzen. Das OVG Lüneburg jedoch verwarf die Berufung der Datenschutzbehörde – nunmehr allerdings mit materiell-rechtlicher Begründung unter Anwendung von § 6b BDSG aF (jetzt § 4 BDSG).

#### 3.1.1 Erforderlichkeit

Die Videoüberwachung, so das OVG, diene der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke nach § 6b Abs. 1 Nr. 3 BDSG aF. Insgesamt erkennt das OVG drei Zwecke an:

- Die Verfolgung von Straftaten bei der Fahrgastbeförderung und die Sicherung von Beweismaterial zu ihrer Aufklärung,[51]
- die Gefahrenabwehr einschließlich der Verhütung von Straftaten,[52]
- die Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste als Nebenzweck.[53]

Das OVG hat keine Zweifel an der Erforderlichkeit einer zeitlich unbegrenzten und ausnahmslos auf allen Fahrstrecken stattfinden Videoüberwachung. Die Erforderlichkeit im Sinne des § 6b Abs. 1 S. 1 BDSG setze voraus, dass das festgelegte Ziel mit der Überwachung tatsächlich erreicht werden könne und es dafür kein anderes, gleich wirksames, aber mit Blick

[50] VG Hannover, Urt. v. 10.2.2016 – 10 A 4379/15, ZD 2016, 349.

[51] OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, BeckRS 2017, 123619, Rn. 29.

[52] Ebenda.

[53] Ebenda, Rn. 38.

auf das Grundrecht der informationellen Selbstbestimmung weniger einschneidendes Mittel gebe. Dabei bestimme sich die Erforderlichkeit, so das OVG, nach objektiven Maßstäben.[54]

Diese objektiven Maßstäbe der Erforderlichkeit sieht das OVG durch das Zahlenmaterial der ÜSTRA über zahlreiche Störungen in ihren Bussen und Bahnen, die ein repressives Tätigwerden veranlasst haben, ausreichend belegt. Aus einer Übersicht über „Sicherheitsrelevante Vorfälle in Fahrzeugen" zwischen März 2009 und Juni 2014 (größtenteils vor Einführung der Videoüberwachung 2013) gehe laut OVG hervor, dass in diesem Zeitraum insgesamt 1740 sicherheitsrelevante Vorfälle erfasst worden seien, wobei die jährlich Anzahl relativ konstant gewesen sei (also etwa 330 Vorfälle pro Jahr). Es handele sich um Ereignisse in den Bereichen Vandalismus (Graffiti, Scheibenkratzen und Scheibeneinschlagen usw.), tätliche Angriffe auf Fahrzeuge, Mitarbeiter und Fahrgäste, verbale Angriffe wie Pöbeleien, Beleidigungen, Belästigungen oder Bedrohungen sowie um schwere Straftaten wie sexuelle Nötigung, Körperverletzung, Raub und Diebstahl.[55]

Das Ergebnis dieser Auswertung sieht das OVG durch eine vorgelegte Aufstellung von 348 Sachverhalten bestätigt, die in dem Zeitraum vom 1. Oktober 2014 bis zum 30. November 2015 Anlass für die Sicherung der Black-Box-Videodaten in den Bussen und Bahnen der Klägerin gegeben habe. Daraus ergäbe sich eine Vielzahl von Störfällen, die sich verteilt auf zahlreiche Bus- und Stadtbahnlinien an unterschiedlichen Wochentagen und zu allen Tages- und Nachtzeiten ereignet hätten. Darunter sind gravierende Straftaten, wie eine Liste mit Beispielen veranschaulicht. Daneben enthält die Aufstellung zahlreiche Aufforderungen zur Videosicherung durch die Polizei wegen diverser Straftatbestände, u.a. wegen eines Tötungsdeliktes, wegen Raubes, wegen Körperverletzung, wegen sexueller Belästigung Minderjähriger und wegen Sachbeschädigung.[56]

Aus dem Zahlenmaterial der ÜSTRA zu Störfällen ergeben sich jedoch entgegen der Ansicht des OVG mehr ungeklärte Fragen als Antworten. Zunächst wird in der Tat belegt, dass es in den Bussen und Bahnen der ÜSTRA ausreichenden Anlass für die genannten Zwecke der Verhütung und Verfolgung von Straftaten gibt. Auch dass es nicht nur wenige Linien gibt, auf die sich die Maßnahmen beschränken könnten, wird deutlich. Aber ob Videoüberwachung das geeignete Mittel hierfür ist, gerät doch sehr in Zweifel. 1740 sicherheitsrelevante Vorfälle in gut 5 Jahren im Wesentlichen vor Einführung der Videoüberwachung und dann 348 Vorfälle in 14 Monaten

[54] Ebenda, Rn. 30.

[55] Ebenda, Rn. 31.

[56] Ebenda, Rn. 32.

nach Einführung erwecken auf den ersten Blick den Eindruck, dass der präventive Effekt der Überwachung gegen Null geht.

Auch daraus, dass in 348 Fällen das Videomaterial aus gegebenem Anlass nicht gelöscht wurde, beweist nicht, dass es tatsächlich bei der Aufklärung von Straftaten hilfreich war. Die Frage der Geeignetheit der Videoüberwachung wird in der gesamten Entscheidung nur kurz mit der bloßen Behauptung gestreift, dass Bildaufzeichnungen die Effektivität der Abschreckung erhöhten, weil der potentielle Täter damit rechnen müsse, dass seine Tat aufgezeichnet und die Aufzeichnung nicht nur für seine Identifizierung, sondern auch als Beweismittel in einem Strafverfahren zur Verfügung stehen werde.[57] Als Beleg führt das OVG nicht etwa kriminologische Untersuchungen tatsächlicher Verhältnisse an, sondern die Reeperbahn-Entscheidung des BVerwG, in der bereits die wortgleiche Annahme unbelegt formuliert wurde.[58] Das von der ÜSTRA laut OVG vorgelegte Zahlenmaterial kann diese Behauptung jedenfalls nicht stützen.

### 3.1.2 Interessenabwägung

Anhaltspunkte für das Überwiegen schutzwürdiger Interessen der Betroffenen sieht das OVG Lüneburg nicht. Die Interessenprüfung gemäß § 6b Abs. 1 und 3 BDSG aF erfordere eine am Verhältnismäßigkeitsgrundsatz orientierte umfassende Abwägung zwischen den durch die Zwecke der Videoüberwachung bestimmten grundrechtlich geschützten Positionen der Anwender von Videotechnik und den Interessen derjenigen, die Objekt der Videoüberwachung und Speicherung der Bilddaten seien.[59] Der Frage der Eingriffsintensität komme eine entscheidende Bedeutung zu.

Dass die Belange, die zu der Videoüberwachung geführt haben, gewichtig sind, steht außer Frage. Insoweit kann der Entscheidung nur zugestimmt werden. Die hohe Zahl gravierender Vorfälle gibt allen Anlass, Maßnahmen zu ergreifen, die möglichst präventiv oder wenigstens repressiv gegenüber Straftaten wirken. Aber auch die Belange der von Überwachung Betroffenen haben großes Gewicht, das das OVG kaum berücksichtigt. Das Gericht gibt selbst den Maßstab vor, wenn es formuliert, dass das Gewicht des Eingriffs maßgeblich durch Art und Umfang der erfassten Informationen, durch Anlass und Umstände der Erhebung, den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt werde. Zu Art und Umfang der erfassten Informationen sollte berücksichtigt werden, dass Bilder, die das Gesicht eines Menschen zeigen, hohe Aus-

[57] Ebenda, Rn. 36.

[58] BVerwG, Urt. v. 25.1. 2012 – 6 C 9/11, NVwZ 2012, 757 (759), Rn. 30.

[59] OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, BeckRS 2017, 123619, Rn. 39.

sagekraft haben und z.B. Emotionen oder sogar bestimmte Gesundheitszustände zeigen können. Zu den Umständen der Erhebung wäre zu berücksichtigen, dass der ÖPNV für viele Menschen keine realistische Alternative hat. Sie müssen den Bus oder die Bahn benutzen. Weiter wäre zu berücksichtigen, dass der betroffene Personenkreis völlig offen ist und auch Kinder einschließt. All dies scheint das Gericht nicht im Blick zu haben.

Das OVG betont, dass den Belangen der Betroffenen, möglichst gering durch die Überwachungsmaßnahmen belastet zu werden, ausreichend dadurch Rechnung getragen werde, dass das Bildmaterial unbesehen lediglich für 24 Stunden gespeichert werde und für den Einzelfall einer Auswertung der Datenträger Zugriffsbeschränkungen bestünden. Die Daten sind in einem gesonderten Raum, der nur von einem vorher schriftlich festgelegten Personenkreis betreten werden darf, auf einem nicht vernetzten Computer abgelegt. Die Zugriffsberechtigten müssten sich bei Aufruf der Daten am Computer mittels einer Eingabe von Benutzerkennung und Passwort legitimieren. Das ist alles gut und wichtig. Aber zu beachten ist auch, dass eine längerfristige Nutzung aus besonderem Anlass gar nicht so selten vorkommt. Denn immerhin ist es nach den Angaben der ÜSTRA in 348 Fällen in 14 Monaten dazu gekommen, dass das Bildmaterial über die Löschfrist hinaus zu Aufklärungszwecken verwendet worden ist.[60]

Besondere Aufmerksamkeit verdient das letzte Argument des OVG, dass die Beförderungsdauer im öffentlichen Nahverkehr relativ gering sei, so dass die Überwachung regelmäßig nicht über einen längeren Zeitraum stattfinde. Hier liegt wohl ein Schlüsselproblem. Jede Interessenabwägung betrachtet zulasten der bildlich Erfassten immer nur die isolierte Maßnahme, die jeweils rechtlich zu überprüfen ist. Das Zusammenspiel mit vielfältigen weiteren Überwachungsmaßnahmen bleibt unberücksichtigt. Dass diejenigen, die das Fahrzeug des ÖPNV verlassen, sofort in den Bereich der nächsten Überwachungsanlage auf dem Bahnsteig oder im Bahnhofsgebäude oder auf dem Bahnhofsvorplatz usw. geraten, wird dem einzelnen Eingriff nicht zugerechnet.

### 3.2 Videoüberwachung in einer Apotheke (OVG Saarlouis)

Nach einer Anordnung der Landesbeauftragten für Datenschutz im Saarland vom 30.7.2014 wird der Eigentümer und Betreiber der S.-Apotheke aufgefordert, u.a. die Videoüberwachung im Verkaufsraum einzustellen Dagegen erhebt dieser Klage, die jedoch im Hinblick auf die drei Kameras im Verkaufsraum ohne Erfolg bleibt. Das VG Saarlouis hat die Klage insoweit abgewiesen, weil es weder eine konkrete noch eine abstrakte Gefähr-

[60] Ebenda, Rn. 42.

dungslage dargelegt sah. Es sei auch nicht nachvollziehbar, dass das festgelegte Ziel einer Reduzierung des Fehlbestands mit der Überwachung tatsächlich erreicht werden könne.[61]

Der Berufung hiergegen gab das OVG Saarlouis statt, weil der Einsatz der Verkaufsraumkameras durch § 6b Abs. 1 i.V.m. Abs. 3 BDSG aF gerechtfertigt sei. Die Videoüberwachung des Verkaufsraumes, mit der sich der Kläger davor schützen möchte, dass in seinem Verkaufsraum Waren gestohlen würden, sei ein Fall der Wahrnehmung des Hausrechts im Sinne von § 6b Abs. 1 Nr. 2 BDSG aF und diene zugleich der Wahrnehmung berechtigter Interessen i.S.v. § 6b Abs. 1 Nr. 3 BDSG. Der Inhaber des Hausrechts sei befugt, die zum Schutz des Objekts und zur Abwehr unbefugten Betretens erforderlichen Maßnahmen zu treffen. Dazu zählte auch die Beweissicherung mittels Videoüberwachung zum Schutz des Eigentums des Apothekers.[62] Er könne sich zusätzlich auf den Tatbestand der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke gemäß § 6b Abs. 1 Nr. 3 BDSG berufen. Allerdings müsse das Interesse objektiv begründbar sein und sich aus einer konkreten Gefahrenlage heraus ergeben. Diese Voraussetzungen sieht das OVG durch die Angaben des Klägers erfüllt. Es sei bereits beim Erwerb der Apotheke von einem Steuerberater und Wirtschaftsprüfer ein außergewöhnlich hoher Schwund und eine schlechte Ertragslage festgestellt worden, was den Schluss auf Diebstähle zugelassen habe. Im Jahr 2011 sei außerdem eine Lagerdifferenz in Höhe von etwa 44.000 Euro zu verzeichnen gewesen. Diese Differenz liege nach Angaben des Klägers über dem für Apotheken üblichen Normbereich.[63]

Die vom Kläger durchgeführte Videoüberwachung sei auch für die Wahrnehmung des Hausrechts und seiner (sonstigen) berechtigten Interessen erforderlich. Entsprechend dem allgemeinen Begriffsverständnis der Erforderlichkeit setze dies voraus, dass die Videoüberwachung für den jeweiligen Zweck geeignet sei und kein milderes Mittel zur Verfügung stehe, mit dem der Zweck ebenso wirksam erreicht werden könne. Es sei, so das OVG, nicht notwendig, die am besten geeignete Alternative zu identifizieren. Von einer Geeignetheit sei bereits dann auszugehen, wenn die Erreichung des maßgeblichen Zwecks sinnvoll gefördert werde. Hierzu sei eine Videobeobachtung des Verkaufsraums der Apotheke in der Lage, weil sie potenzielle Täter von der Begehung von Diebstählen abschrecke. Es entspräche allgemeiner Lebenserfahrung, dass die Wahrscheinlichkeit, dass derartige Taten begangen würden, umso geringer sei, je höher das Risiko sei, entdeckt und zur Verantwortung gezogen zu werden. Nicht ausschlaggebend sei es,

[61] VG Saarlouis, Urt. v. 29.1.2016 – 1 K 1122/14, ZD 2016, 549 (550 f.), Rn. 37 f. und 49.

[62] OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, BeckRS 2017, 137554, Rn. 34.

[63] Ebenda, Rn. 36.

dass seit der Installation der Kameras im Jahr 2008 den Angaben des Klägers zufolge weiterhin ein nicht aufzuklärender Warenschwund zu verzeichnen sei. Denn für die Geeignetheit komme es nicht darauf an, dass solche Vorfälle auch in Zukunft nicht gänzlich unterbunden werden könnten.[64]

Die Kameras existieren also seit 2008. Dennoch wird eine Lagerdifferenz des Jahres 2011 herangezogen, um die Erforderlichkeit der Kameras zu begründen. Ansonsten wird ähnlich wie im Fall des OVG Lüneburg eine allgemeine Mutmaßung über die Wirksamkeit der Videoüberwachung für aussagekräftiger gehalten als das Zahlenmaterial.

Als mildere, gleich wirksame Mittel zur Zweckerreichung zieht das OVG die Beschäftigung von Wachpersonal in Betracht. Dies sei dem Kläger jedoch wirtschaftlich nicht zumutbar. Die Überwachung des Verkaufsraumes durch eigene Mitarbeiter des Klägers stelle keine gleich geeignete Maßnahme dar, da diese überwiegend mit der Beratung und Bedienung der Kunden beschäftigt seien.[65] Diese Aussage ist durchaus gewagt, da über den Grad der Eignung der Videoüberwachung im vorliegenden Fall aus den Angaben des Klägers wenig bekannt ist. Mögliche mildere Mittel, die die Art der Präsentation der Ware im Selbstbedienungsbereich betreffen, werden nicht in Betracht gezogen.

Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der Betroffenen liegen aus Sicht des OVG nicht vor. Die Intensität des Eingriffs in die Rechte von erfassten Kunden sei im Einzelfall nicht als hoch anzusehen. Der Besuch einer Apotheke sei weder ehrenrührig noch stelle er ein Indiz für das Vorliegen einer Erkrankung i.S. eines sensiblen Gesundheitsdatums dar.[66] Das OVG macht sich dann noch Gedanken, ob Rezepte oder Verpackungen von Medikamenten, die Personen entgegennehmen, sensible Daten offenbaren könnten. Letztlich stellt es aber fest, dass die Videoaufnahmen nur zeigten, was ein beliebiger Beobachter, also auch ein anderer Apothekenbesucher ebenfalls sehen würde. Die nur theoretisch bestehende Möglichkeit, aufgezeichnete Videos ohne ausreichenden Grund weiterzugeben oder im Internet zu veröffentlichen, führte für sich genommen nicht zur Unzulässigkeit, da andernfalls Videoaufzeichnungen, welche § 6b BDSG ausdrücklich erlaube, praktisch generell nicht mehr möglich wären.[67]

---

[64] Ebenda, Rn. 37.

[65] Ebenda, Rn. 38.

[66] Ebenda, Rn. 40.

[67] OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, BeckRS 2017, 137554, Rn. 40.

Ähnlich wie in der Entscheidung des OVG Lüneburg wird auch hier nicht im Einzelnen betrachtet, was Videoaufnahmen von Menschen im SB-Verkaufsbereich einer Apotheke an sehr persönlichen Informationen offenbaren können. Für sich genommen handelt es sich sicherlich um belanglose Daten. Fragt sich also, wie sicher technisch gewährleistet ist, dass die Daten wieder gelöscht werden, ohne dass sie mit anderen Daten zusammengeführt werden können. Werden die Daten vom Internet getrennt gespeichert oder werden sie mit Hilfe des Netzes ausgewertet. Schließlich können sie ihren Zweck ja nur optimal erfüllen, wenn das Datenmaterial von drei Kameras auch tatsächlich gesichtet wird.

### 3.3 Dashcam-Aufnahmen als Beweismittel (BGH)

Die Dashcam-Entscheidung des BGH ist in Deutschland auch in den allgemeinen Medien stark beachtet worden. Hier sollen nur wenige Aspekte herausgegriffen werden, die für die Fragen der Erforderlichkeit und Interessengerechtigkeit besonders interessant sind. Der Kunstgriff des BGH besteht darin, zwei Abwägungsentscheidungen durchzuführen. Im ersten Schritt wird geklärt, ob der Dashcam-Einsatz des Klägers auf § 6b Abs. 1 BDSG aF bzw. auf § 28 Abs. 1 Nr. 2 BDSG aF (der BGH lässt dies offen) gestützt werden kann oder als datenschutzwidrig zu betrachten ist.[68] Im zweiten Schritt wird in einer Güterabwägung zwischen den Interessen der Beteiligten ermittelt, ob datenschutzwidrig erlangtes Beweismaterial im Zivilprozess als Beweismittel verwertet werden kann.[69]

§ 6b Abs. 1 BDSG aF bzw. § 28 Abs. 1 Nr. 2 BDSG aF verlangen nach Ansicht des BGH die Erforderlichkeit der Datenerhebung im Sinne eines zumutbaren mildesten Mittels. Für den Zweck der Sicherung von Beweismitteln im Fall eines Verkehrsunfalls sei es technisch möglich, die dauerhafte Aufzeichnung zu vermeiden und lediglich eine kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen vorzunehmen. Der BGH setzt sich recht eingehend mit technischen Alternativen auseinander und kommt zu dem Schluss, dass die vorhandenen technischen Möglichkeiten, die Persönlichkeitsrechte Dritter zu schützen („Privacy by design“), hier nicht genutzt worden seien. Dies führe zu einem Überwiegen der schutzwürdigen Interessen der anderen Verkehrsteilnehmer. Weil technisch mögliche Einschränkungen zur Verkürzung der Aufzeichnungsdauer und Verknüpfung der Speicherung mit einem konkreten Aufzeichnungsanlass nicht gegeben waren, sei eine weitere Prüfung nicht erforderlich und für den Streitfall von einer Unzulässigkeit der Aufnahmen auszugehen.[70]

---

[68] BGH, Urt. v. 15.5.2018 – V ZR 233/17, NJW 2018, 2883 (2885), Rn. 25 ff.

[69] BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2888), Rn. 39 ff.

[70] BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2885), Rn. 24 ff.

Der BGH zeigt sich recht aufgeschlossen gegenüber Befürchtungen, dass Missbrauch mit den Videoaufnahmen getrieben wird. Er betont, dass die im Fahrzeug des Klägers installierte Kamera regelmäßig über einen Zeitraum von ca. vier Stunden ohne konkreten Anlass Aufnahmen gemacht habe, nicht nur für den Fall eines Unfalls. Die vorgelegte 40 Sekunden lange Aufnahme sei Teil einer davor begonnenen Aufzeichnung. Durch eine solche permanente Aufzeichnung werde regelmäßig eine Vielzahl von Personen in kurzer Zeit in ihrem allgemeinen Persönlichkeitsrecht betroffen. Es werde festgehalten, wann ein Betroffener sich an einem bestimmten Ort, mit welchem Verkehrsmittel, gegebenenfalls in welcher Begleitung oder in welcher Verfassung aufhalte. Eine weite Verbreitung dieser Aufzeichnungsmöglichkeiten durch Dashcams im Straßenverkehr könnte bei entsprechender technischer Gestaltung bis hin zur Erstellung von Bewegungsprofilen zahlreicher Verkehrsteilnehmer ausgebaut werden und den Aufenthalt in der Öffentlichkeit unter einen dauernden Überwachungsdruck stellen, insbesondere durch die Speicherung, Zusammenführung und bleibende Verfügbarkeit der Aufnahmen. Diese Daten würden aber für eine Unfallrekonstruktion größtenteils nicht benötigt.[71]

Im Unterschied zum OVG Saarlouis lässt der BGH also den möglichen Missbrauch als einzubeziehende Gefahr gelten und verlangt bei der Frage milderer Mittel, technische Varianten in Betracht zu ziehen. Erforderlich ist das zumutbare mildeste Mittel, das auch nicht unbedingt gleichermaßen geeignet sein muss, solange es den Zweck zumutbar erfüllt.

Bei der zweiten Abwägung zwischen dem Beweisverwertungsinteresse des Klägers und den Persönlichkeitsrechten des Beklagten, klammert der BGH hingegen mögliche Eingriff in die allgemeinen Persönlichkeitsrechte anderer Verkehrsteilnehmer, Fußgänger, Radfahrer oder anderer Kraftfahrer bzw. Insassen aus. Denn ihrem Schutz sei vor allem durch die Regelungen des Datenschutzrechts Rechnung zu tragen. Zwar sei nicht zu verkennen, dass die Möglichkeit einer Beweisverwertung Anreize für die Nutzung von Dashcams setzen könne, doch sei ihr Gefahrenpotential nicht im Zivilprozess einzugrenzen oder (zusätzlich) zu sanktionieren, auch wenn sich der Senat generalpräventiven Erwägungen nicht immer gänzlich verschlossen habe. Deshalb sei es für die Frage der Verwertbarkeit des Beweismittels nicht von Bedeutung, dass der Teil der Aufzeichnung, der nicht im Prozess vorgelegt worden oder für die Unfallrekonstruktion nicht erheblich sei, möglicherweise zu Eingriffen in das allgemeine Persönlichkeitsrecht dritter Personen führe.[72] Letztlich ist es auch hier die isolierte Betrachtung des

[71] BGH, Urt. v. 15.5.2018 – V I ZR 233/17, NJW 2018, 2883 (2886), Rn. 26.

[72] BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2890), Rn. 52.

einzelnen Betroffenen hinsichtlich einer einzelnen Maßnahme, die den Eingriff auf ein zu vernachlässigendes Maß schrumpfen lässt.

### 3.4 Ergebnisse

Die Eignung der Videoüberwachung im Sinne einer verbesserten Verhütung und Verfolgung von Straftaten wird von den Gerichten auch in Fällen angenommen, in denen eine entsprechende Wirkung in den vorgelegten Zahlen nicht zu erkennen ist. Es genügt den Gerichten, dass sich die abschreckende Wirkung der Videoüberwachung aus allgemeiner Lebenserfahrung ergeben soll. Das kommt einer Beweislastumkehr zulasten der informationellen Selbstbestimmung gleich. Die Datenschutzbehörde sieht sich damit in der Lage, darlegen und beweisen zu müssen, dass die Videoüberwachung nicht wirkt.

Mildere Mittel werden in den OVG-Entscheidungen nur sehr eingeschränkt in Betracht gezogen. Dies könnte sich mit der Dashcam-Entscheidung des BGH ändern. Denn hier führt der Verzicht auf eine technische Alternative dazu, dass der Einsatz der Dashcam als datenschutzwidrig eingestuft wird. Danach ist zu erwarten, dass „Privacy by Design"-Erwägungen künftig eine zentrale Rolle in entsprechenden Konflikten einnehmen werden.

Ob eine weniger in die Rechte der bildlich Erfassten eingreifende technische Lösung wirklich die gleiche Wirksamkeit aufweisen muss, ist nach der Dashcam-Entscheidung des BGH fraglich. Auch eine zumutbar geringere Wirkung könnte ausreichen. Auf jeden Fall käme es auf tatsächlich festgestellte Wirkungen an, um einen solchen Vergleich durchzuführen.

Es gibt eine Tendenz bei der Interessenabwägung, die Risiken auf der Seite der bildlich Erfassten kleinzureden. Allerdings besteht hier unverkennbar ein strukturelles Problem. Tatsächlich stehen sich hier sehr unterschiedliche Gefährdungen gegenüber, die schwer gegeneinander aufzurechnen sind. Der Punkt, an dem die Waage plötzlich zur anderen Seite ausschlagen soll, entzieht sich jeder Veranschaulichung. Also wird in einer Urteilsbegründung zwangsläufig eine Seite runtergespielt. Das gelingt bei Belangen der Privatsphäre und der informationellen Selbstbestimmung leichter als beim Schutz von Eigentum, Leib und Leben. Denn die Verletzung der Privatsphäre ist weit weniger fassbar, psychisch vermittelt und in geringen Dosen auch leicht zu ertragen. Erst wenn man den Zusammenhang herstellt zu den vielen weiteren Beeinträchtigungen der Privatsphäre durch zahlreiche weitere Überwachungskameras, zu Datenlecks und Datenmissbrauch bekommt die Beeinträchtigung der Privatsphäre Gewicht. Im einzelnen Gerichtsverfahren steht aber regelmäßig nur ein kleiner Ausschnitt zur Entscheidung, der gegen die Risiken gefährlicher Straftaten nicht bestehen kann.

# 4 Neue Rechtslage in Deutschland seit Anwendung der DSGVO

In Deutschland existierte bereits seit Mai 2001 die spezielle Vorschrift § 6b Abs. 1 BDSG a.F. zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen. Sie beschränkte die Zulässigkeit solcher Einrichtungen auf eine Beobachtung, die entweder zur Aufgabenerfüllung öffentlicher Stellen oder – im Hinblick auf private Stellen – zur Wahrnehmung des Hausrechts bzw. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Außerdem dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Daneben sind spezifische Bestimmungen zur Kennzeichnungspflicht der Videobeobachtung in § 6b Abs. 2 BDSG a.F. getroffen worden. Bei Anwendungsbeginn der DSGVO am 25. Mai 2018 will der deutsche Gesetzgeber weiterhin an einer nationalen Regelung zur Videoüberwachung öffentlich zugänglicher Räume festhalten und schafft hierzu in § 4 des neuen Bundesdatenschutzgesetzes Bestimmungen, die weitgehend der alten Regelung in § 6b BDSG aF entsprechen.[73] Wegen des Anwendungsvorrangs der DSGVO wird jedoch bestritten, dass das nationale Recht auf private Videoanlagen im öffentlichen Raum weiter anzuwenden ist.

## 4.1 Vorrang der DSGVO bei privater Videoüberwachung

Nicht in Frage steht, dass das nationale Recht zur Videoüberwachung für die Überwachungsanlagen öffentlicher Stellen weiterhin maßgeblich ist. Neben dem neuen § 4 BDSG kommt für öffentliche Stellen die Anwendung zahlreicher spezialgesetzlicher Regelungen auf Bundes- und vor allem auf Landesebene in Betracht. So können sich die Strafverfolgungsbehörden auf § 100h Abs. 1 Nr. 1 StPO stützen. Auch sind in den Landesdatenschutzgesetzen bzw. Landespolizeigesetzen flächendeckend weitere einschlägige Erlaubnisnormen zu finden. Öffentliche Stellen können alle diese nationalen Regelungen auch nach dem 25. Mai 2018 problemlos anwenden, da dafür die Öffnungsklausel in Art. 6 Abs. 3 S. 1 lit. b i.V.m. Abs. 1 S. 1 lit. e DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) in Anspruch genommen werden kann.

Bei nichtöffentlichen Stellen jedoch kommt diese Öffnungsklausel nicht zum Zuge, da regelmäßig nichtöffentliche Interessen vertreten werden oder, selbst wenn private Videoüberwachung öffentlichen Interessen dienen könnte, es bei Privaten an der in lit. e vorausgesetzten Übertragung der Aufgaben auf diese fehlt.[74] Vielmehr geht es bei der Videoüberwachung

[73] *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 1.

[74] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 23.

durch Private vorrangig um deren berechtigte Interessen, für die gerade Art. 6 Abs. 1 S. 1 lit. f DSGVO ohne eine Öffnungsklausel geschaffen worden ist. Ganz überwiegend ist daher vertreten worden, dass § 4 Abs. 1 S. 1 Nr. 2 und 3 BDSG für nichtöffentliche Stellen unionsrechtswidrig ist und unangewendet bleiben muss.[75]

Dieser Auffassung hat sich am 27. März 2019 auch das Bundesverwaltungsgericht angeschlossen.[76] Für eine künftige Anwendung des § 4 Abs. 1 S. 1 BDSG n.F. auf die Videoüberwachungen privater Verantwortlicher sei laut BVerwG kein Raum. Die Öffnungsklauseln des Art. 6 Abs. 2 und 3 DSGVO für Verarbeitungen im öffentlichen Interesse nach Art. 6 Abs. 1 lit. e DSGVO erfasse die Videoüberwachungen privater Verantwortlicher nicht. Denn eine Privatperson könne sich nicht selbst zum Sachwalter des öffentlichen Interesses erklären. Damit sei die Videoüberwachungen privater Verantwortlicher nunmehr an Art. 6 Abs. 1 lit. f DSGVO zu messen. Damit ist der Streitpunkt zugunsten des Vorrangs der DSGVO von höchstrichterlicher Stelle überraschend schnell geklärt worden.

### 4.2 Änderungen durch die DSGVO im Überblick

In materieller Hinsicht bestehen allerdings ohnehin weitgehend identische Regelungsgehalte im nationalen Recht des § 4 Abs. 1 S. 1 Nr. 3 BDSG einerseits und im europäischen Recht des Art. 6 Abs. 1 S. 1 lit. f DSGVO andererseits.[77] Unterschiede mögen sich bei den Modalitäten der Kennzeichnungspflicht zeigen, die an dieser Stelle jedoch nicht betrachtet werden sollen. Die Fragen der materiellen Rechtfertigung jedenfalls stellen sich nach dem BDSG und der DSGVO nahezu identisch dar, wie auch das BVerwG[78] bestätigt: a) berechtigtes Interesse an der Überwachung, b) hierfür Erforderlichkeit der Überwachung, c) kein Überwiegen der Interessen erfasster Personen. Bevor auf diese drei Kernpunkte der Prüfung von Maßnahmen der Videoüberwachung näher eingegangen wird, sei noch kurz auf vier Besonderheiten der Anwendung der DSGVO im Vergleich zum hergebrachten deutschen Recht hingewiesen.

---

[75] *Brink/Wilhelm*, in: Wolff/Brink, BeckOK DatenschutzR, BDSG, § 4 Rn. 19; *Buchner/Petri*, in: Kühling/Buchner, DSGVO/BDSG, DSGVO, Art. 6 Rn. 172; *Grabenschröer/Reuter*, in: Taeger/Gabel, DSGVO/BDSG, BDSG, § 4 Rn. 43; *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 24; *Starnecker*, in: Gola/ Heckmann, BDSG, § 4 Rn. 11; a.A. *Schwartmann/Jacquemain*, in: Schwartmann/Jaspers/ Thüsing/Kugelmann, DSGVO/BDSG, DSGVO, Anh. zu Art. 6 Rn. 2 ff.

[76] BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, BeckRS 2019, 9874, Rn. 44 ff.

[77] *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 12; *Datenschutzkonferenz (DSK)*, Kurzpapier Nr. 15 „Videoüberwachung nach der Datenschutz-Grundverordnung“, S. 2.

[78] BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, BeckRS 2019, 9874, Rn. 47.

Erstens kann die Überwachung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO ausdrücklich auch im berechtigten Interesse Dritter stattfinden. In § 4 Abs. 1 S. 1 Nr. 3 BDSG ist dies nicht ausdrücklich vorgesehen, sondern es fehlt eine Spezifizierung. Im Sinne einer europarechtskonformen Auslegung sind aber auch nach § 4 Abs. 1 S. 1 Nr. 3 BDSG die berechtigten Interessen Dritter einzubeziehen. Zweitens sieht Art. 6 Abs. 1 S. 1 lit. f DSGVO ausdrücklich vor, dass es bei der Interessenabwägung besonders zu berücksichtigen ist, wenn die betroffene Person ein Kind ist. Da Videoüberwachungsanlagen in aller Regel auch Kinder erfassen, ist die Norm hier relevant. Abgeleitet wird hieraus ein erhöhter Sorgfaltsmaßstab bei der Prüfung,[79] der allerdings auch schon nach altem Recht bestanden haben dürfte. Eine Rolle spielen könnte für den Prüfungsmaßstab der DSGVO drittens, dass nach dem ErwG 47 die vernünftigen Erwartungen der betroffenen Personen bei der Interessenabwägung zu berücksichtigen sein sollen. Entgegen des strikt objektiven Ansatzes des alten Rechts soll nunmehr ein subjektives Element in die Interessenabwägung einfließen, wonach zusätzlich relevant wird, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.[80]

Die größten Auslegungsschwierigkeiten bereitet die vierte zu erörternde Abweichung der DSGVO vom alten Recht der Videoüberwachung. Die DSGVO schützt in Art. 9 verstärkt Daten mit besonders sensiblen Informationen.[81] Es geht um die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Selbstverständlich enthalten auch Bilddaten, die eine Videoüberwachungsanlage verarbeitet, unausweichlich derartige Informationen, die sich z.B. aus der Hautfarbe, aus dem Gangbild oder aus religiösen Kennzeichen ergeben können. Die kontrovers geführte Diskussion,[82] wie sich dies auf den Prüfungsmaßstab der Videoüberwachung auswirkt, kann hier nicht entschieden werden. Ähnlich wie beim oben genannten besonderen Schutz von Kindern wird aber mit Rücksicht auf Art. 9

---

[79] *Schulz*, in: Gola, DSGVO, Art. 6 Rn. 59; *Taeger*, in: Taeger/Gabel, DSGVO/BDSG, DSGVO, Art. 6 Rn. 99.

[80] *Datenschutzkonferenz (DSK)*, Kurzpapier Nr. 15 „Videoüberwachung nach der Datenschutz-Grundverordnung“, S. 2.

[81] *Mester*, in: Taeger/Gabel, DSGVO/BDSG, DSGVO, Art. 4 Rn. 1.

[82] *Reuter*, ZD 2018, S. 564; *Schneider/Schindler*, ZD 2018, S. 463; *Schwenke*, NJW 2018, S. 823 (825).

DSGVO mindestens erhöhte Sorgfalt der gesamten Prüfung zu verlangen sein.

## 5 Erforderlichkeit und Interessengerechtigkeit unter Anwendung der DSGVO

Drei Fragen bilden den materiell-rechtlichen Kern gerichtlicher Entscheidungen zur Videoüberwachung in öffentlich zugänglichen Räumen. Das BVerwG[83] spricht in seiner jüngsten Entscheidung zwar von einem nur zweistufigen Prüfprogramm gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO. Das liegt allerdings schlicht daran, dass in der Vorschrift zwei Fragen im ersten Halbsatz zusammengefasst sind. Auf der ersten Stufe wird also erstens geklärt, ob berechtigte Interessen für die Videoüberwachung gegeben sind. Zweitens wird auf dieser Stufe geprüft, ob die jeweilige Überwachungsmaßnahme für die jeweiligen Interessen erforderlich ist. Auf der zweiten Stufe findet eine Interessenabwägung zwischen den Belangen der Beteiligten statt. Diese insgesamt drei Kernfragen der juristischen Prüfung gilt es, nachfolgend näher zu untersuchen.

### 5.1 Berechtigte Interessen

In der jüngsten Entscheidung des BVerwG vom 27. März 2019 hat dieses festgestellt, dass berechtigte Interessen, die eine Videoüberwachung durch Private erlauben können, schutzwürdig und objektiv begründbar sein müssen.[84] Die Verhinderung und Aufklärung von Straftaten stelle grundsätzlich ein solches Interesse dar. Objektiv begründbar sei es jedoch nur, wenn auf Grundlage von tatsächlichen Erkenntnissen eine Gefährdungslage bestehe, die über das allgemeine Lebensrisiko hinausgehe.[85] In Betracht zog das BVerwG, ob die Arztpraxis, um deren Überwachung es ging, in einem Gebiet mit erhöhtem Gefahrenpotenzial gelegen sei oder ob sich Straftaten bereits ereignet hätten. Mangels derartiger Tatsachen scheiterte das genannte Interesse bereits beim ersten Prüfpunkt.[86]

Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann nach Ansicht des *Düsseldorfer Kreises* der unabhängigen Datenschutzbehörden ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, sei darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen

[83] BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, BeckRS 2019, 9874, Rn. 47.

[84] Ebenda, Rn. 47.

[85] Ebenda, Rn. 28.

[86] Ebenda, Rn. 29.

werden könne.[87] Neben präventiven Zwecken kommen auch die Verfolgung von Straftaten und die Beweissicherung zur Durchsetzung zivilrechtlicher Schadensersatzansprüche als berechtigte Interessen grundsätzlich in Betracht.[88] Zu fordern seien konkrete Tatsachen, aus denen sich eine Gefährdung ergebe, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Die erhöhte Gefahrenlage kann sich auch aus einer typisierten Betrachtung ergeben, sofern sich diese objektiv begründen lässt.[89] Zum Schutz von Leben, Gesundheit und bedeutenden Sach- und Vermögenswerten soll eine nach allgemeiner Lebenserfahrung typischerweise gefährliche Sachlage ausreichen, die man bei Tankstellen, aber auch bei Juwelieren oder Banken häufig bejahen könne.[90] Hier könne Videotechnik installiert werden, bevor Taten begangen worden seien.

Für die in § 4 Abs. 1 BDSG genannten öffentlich zugänglichen großflächigen Anlagen sowie Fahrzeugen und zugänglichen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs unterstellt der Gesetzgeber, dass der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen ein besonders wichtiges Interesse darstelle.[91] Das berechtigte Interesse wird für diese Bereiche vermutet.[92] Nach der Entscheidung des BVerwG vom 27. März 2019[93] ist diese Regelung auf die Videoüberwachung privater Verantwortlicher jedoch wegen des Vorrangs der DSGVO nicht mehr anzuwenden.

Grundsätzlich kommt Videotechnik also für das Interesse der Verhütung und Verfolgung von Straftaten in Betracht. Der Umstand, dass nach den vorliegenden Studien bei diesen Zwecken immer nur Teilerfolge möglich sind und unter Umständen auch diese ausbleiben (siehe 2.1), disqualifiziert Videotechnik nicht von vornherein. Richtig eingesetzt kann sie einen wertvollen Beitrag zur Abschreckung und Verfolgung von Straftaten leisten. Zustimmung und Erwartungshaltung hinsichtlich der Wirkung sind

---

[87] *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, S. 7 f.; ähnlich *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 77.

[88] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 78.

[89] *Becker*, in: Plath, DSGVO/BDSG, BDSG, § 4 Rn. 17; *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 38.

[90] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 76.

[91] *Gola*, in: Gola, DSGVO, Art. 6 Rn. 166.

[92] *Becker*, in: Plath, DSGVO/BDSG, BDSG, § 4 Rn. 18.

[93] Ebenda, Rn. 47.

allerdings in der Bevölkerung sehr hoch (siehe 1.2), so dass ein übertriebener Einsatz ins Blaue hinein nicht ausgeschlossen werden kann.

Bei diesem ersten Punkt der Prüffolge einer Videoüberwachung durch einen privaten Verantwortlichen muss sich dieser klar werden, was er eigentlich sinnvoll erreichen will. Die Zwecke sind bereits zu Beginn der Maßnahme konkret, nicht nur in Schlagworten, festzulegen. Das ergibt sich aus Art. 5 Abs. 1 lit. b DSGVO.[94] Dabei müssen objektive Tatsachen, die das Interesse legitimeren, vorliegen.

### 5.2 Erforderlichkeit

Die Videoüberwachung muss zur Erreichung des ermittelten Zwecks erforderlich sein. Die Erforderlichkeit einer Videoüberwachungsmaßnahme setzt nach vielfach geäußerter Meinung[95] voraus, dass die Maßnahme an sich geeignet ist und kein gleich geeignetes, milderes Mittel zur Zielerreichung existiert.

Zunächst interessiert also die Eignung der Maßnahme. Hier soll es genügen, wenn das Ziel – etwa die Verhütung von Straftaten - durch die Überwachungsmaßnahme gefördert wird; die am besten geeignete Alternative werde nicht verlangt.[96] Wirkungslos im Sinne des verfolgten Zweckes, darf die Videoüberwachung allerdings nicht sein. In der ausgewerteten Rechtsprechung wird das Problem der Eignung mit der allgemeinen Mutmaßung erledigt, dass Bildaufzeichnungen die Effektivität der Abschreckung erhöhten, weil der potentielle Täter damit rechnen müsse, dass seine Tat aufgezeichnet und die Aufzeichnung nicht nur für seine Identifizierung, sondern auch als Beweismittel in einem Strafverfahren zur Verfügung stehen werde.[97] Tatsächlich ist jedoch die Eignung der Videoüberwachung für die Verhütung oder Verfolgung von Straftaten äußerst ungewiss. Soweit Untersuchungen vorhanden sind, schwanken deren Aussagen sehr stark zwischen einem Befund völliger Wirkungslosigkeit und dem einer Verhütung von um die 50 % der Straftaten. Richtigerweise wird daher betont, dass es

---

[94] *Voigt*, in: Taeger/Gabel, DSGVO/BDSG, DSGVO, Art. 5 Rn. 23 ff.

[95] *Becker*, in: Plath, DSGVO/BDSG, BDSG, § 4 Rn. 20; *Gola*, in: Gola, DSGVO, Art. 6 Rn. 168; *Grabenschröer/Reuter*, in: Taeger/Gabel, DSGVO/BDSG, BDSG, § 4 Rn. 48 f.; *Grages/Plath*, CR 2017, S. 791 (794); *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 42; OVG Lüneburg, Urt. v. 29.9.2014 – 11 LC 114/13, ZD 2014, 636 (639); OVG Saarlouis, Urt. v. 14.12.2017, 2 A 662/17, ZD 2018, 134 (135) Rn. 37.

[96] *Becker*, in: Plath, DSGVO/BDSG, BDSG, § 4 Rn. 20; *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 42; OVG Saarlouis, Urt. v. 14.12.2017, 2 A 662/17, ZD 2018, 134 (135) Rn. 37.

[97] OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, BeckRS 2017, 123619, Rn. 36; ähnlich OVG Saarlouis, Urt. v. 14.12.2017 – 2 A 662/17, BeckRS 2017, 137554, Rn. 37.

auf die objektive Prüfung der Umstände der konkreten Maßnahme ankommt.[98] Es muss im Einzelfall gezeigt werden, dass die bildlich Erfassten nicht von einer sinnlosen Maßnahme belastet werden. Soweit dies im Vorfeld einer Maßnahme nicht geklärt werden kann, muss der Erfolg getestet werden. Stellt sich kein oder nur ein marginaler Erfolg der Videoüberwachung ein, ist diese abzubrechen oder wirksamer zu gestalten.

Weiter interessiert, ob es alternative Maßnahmen gibt, die zur Erreichung des Zwecks gleich geeignet sind wie die Videoüberwachung, aber Betroffene nicht oder geringer in ihren Rechten beeinträchtigen. In der Literatur wird vor allem betont, dass die alternativen Maßnahmen auch zumutbar sein müssen und nicht etwa unzumutbare Investitionen verlangen.[99] Das soll vor allem für die Alternative Personal statt Überwachungstechnik gelten. Auch hier kommt es aber auf die konkreten Umstände des Einzelfalls an. Es muss vor allem auch gefragt werden, ob tatsächlich die schonendste wirksame Videotechnik eingesetzt wird.[100] Der BGH[101] hat als milderes Mittel unter dem Stichwort „Privacy-by-Design" verlangt, dass die vorhandenen technischen Möglichkeiten, die Persönlichkeitsrechte Dritter zu schützen, zu nutzen sind. Die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens durch eine Dashcam wurde deswegen für datenschutzwidrig befunden. Insbesondere ist es für die Rechte der von einer Videoüberwachungsanlage bildlich Erfassten sehr risikoreich, wenn die Überwachungsanlage mit dem Netz verbunden ist und daher gehackt werden kann oder die Bilder zur Auswertung gar ins Netz hochgeladen werden. Hier wäre auf jeden Fall die Offline-Variante das mildere Mittel.

Dabei wird auch eine Rolle spielen, ob die Alternative wirklich mindestens gleich geeignet ist. Auch hier kann nicht mit Mutmaßungen gearbeitet werden. Will man nur eine gleich geeignete Alternative zulassen, muss zunächst geklärt werden, wie hoch denn der Wirkungsgrad der tatsächlich eingesetzten Anlage ist. Denn allein der Umstand, dass die in Betracht gezogene Alternative Defizite hat und das Ziel nicht vollständig erreicht, heißt nicht, dass sie weniger geeignet ist. Bei der Verhütung von Straftaten gibt es keine perfekten Instrumente. Im Dashcam-Fall jedenfalls scheint der

98 *Grabenschröer/Reuter*, in: Taeger/Gabel, DSGVO/BDSG, BDSG, § 4 Rn. 48; *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 43.

99 *Taeger*, in: Taeger/Gabel, DSGVO/BDSG, DSGVO, Art. 6 Rn. 112; ähnlich *Becker*, in: Plath, DSGVO/BDSG, BDSG, § 4 Rn. 21; *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 42.

100 Zum Black-Box-Verfahren siehe *Grages/Plath*, CR 2017, S. 791.

101 BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2885), Rn. 25 ff.

BGH in Kauf zu nehmen, dass Alternativen etwas weniger, aber ausreichend geeignet sind.[102]

### 5.3 Interessenabwägung

Sowohl Art. 6 Abs. 1 S. 1 lit. f DSGVO als auch § 4 Abs. 1 S. 1 BDSG verlangen als weiteren Prüfungsschritt der Videoüberwachung eine Interessenabwägung. Laut BVerwG komme es darauf an, ob die Abwägung im jeweiligen Einzelfall ergebe, dass berechtigte Interessen des Verantwortlichen höher zu veranschlagen seien als das informationelle Selbstbestimmungsrecht des Betroffenen.[103] In der Kommentarliteratur heißt es weiter, dass eine umfassende Abwägung aller widerstreitenden Interessen auf Grundlage der konkreten Überwachungssituation vorgenommen werden müsse.[104] Das Gewicht des Eingriffs durch die Überwachung werde maßgeblich durch Art und Umfang der erfassten Informationen, durch Anlass und Umstände der Erhebung, den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.[105]

Die Interessen bzw. Grundrechte und Grundfreiheiten der Betroffenen überwiegen zweifellos dann, wenn durch die Videoüberwachung höchstpersönliche Bereiche der Intimsphäre bildlich erfasst werden, etwa durch die Überwachung von Toiletten, Umkleidekabinen, Duschen oder medizinischen Behandlungsräumen.[106] Ein erhöhter Schutz der Privatsphäre kann auch dort erwartet werden, wo sich Menschen entspannen und erholen wollen: z.B. am Strand, im Bad, im Restaurant, im Biergarten, im Park.[107] Beobachtungsdruck wäre hier sehr störend. Außerdem halten sich die Menschen hier vergleichsweise lange auf und geben zwangsläufig mehr an Bildinformationen preis. Daher überwiegen die Belange der Betroffenen in der Regel. Das mag sich im Einzelfall ändern, wenn sich z.B. ein Park zum Kriminalitätsschwerpunkt entwickelt.

Ein weiterer Grund für den Wunsch nach Privatheit in der Öffentlichkeit liegt in der Gefahr, dass die häufig sehr aussagekräftigen Bilddaten von Hackern entwendet und fremden Zwecken zugeführt werden. Insoweit wächst

---

102 BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2885), Rn. 26.

103 BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, BeckRS 2019, 9874, Rn. 47.

104 *Starnecker*, in: Gola/Heckmann, BDSG, § 4 Rn. 45.

105 OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, BeckRS 2017, 123619, Rn. 39; ähnlich *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, S. 9.

106 *Gola*, in: Gola, DSGVO, Art. 6 Rn. 169.

107 *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, DatenschutzR, DSGVO, Art. 6 Anh. 1 Rn. 107.

die Gefahr, wenn Daten unterschiedlicher Quellen - u. U. durch automatisierte Identitätserkennung personalisiert - zusammengefügt werden. Dem Betroffenen kann nicht entgegengehalten werden, dass er sich schließlich freiwillig in die Öffentlichkeit begeben hat. Denn der Aufenthalt in öffentlichen Räumen ist aus verschiedenen Gründen lebensnotwendig und unausweichlich. Verhältnismäßig können daher nur solche technischen Anlagen sein, die ein Maximum an Sicherheit gegenüber dem Zugriff Unbefugter gewährleisten. Gefordert ist insbesondere,[108] dass der Kreis der Zugriffsberechtigten klein und zuverlässig ist, das Löschen nach kurzer Zeit automatisiert erfolgt und keine Verbindung zum Internet besteht. Wenn Anlagen, die diesen Anforderungen nicht gerecht werden, nicht schon am Tatbestandsmerkmal der Erforderlichkeit gescheitert sind, werden sie bei der Interessenabwägung erneut auf die Probe gestellt. Ergebnis der Interessenabwägung kann auch sein, dass ein hochwirksames Überwachungssystem wegen der hohen Eingriffstiefe gegen ein weniger wirksames zu tauschen ist.

## 6 Bilanz und Perspektiven

Zwei aktuelle Urteile des höchsten deutschen Zivilgerichts (BGH)[109] und des höchsten deutschen Verwaltungsgerichts (BVerwG)[110] machen deutlich, dass die Rechtsprechung – jedenfalls bei der Videoüberwachung durch private Verantwortliche – künftig präziser untersucht haben will, ob Interessen, die den jeweiligen Einsatz rechtfertigen sollen, objektiv gegeben sind, ob sie den Einsatz tatsächlich erforderlich machen und unabhängig davon das Interesse an informationeller Selbstbestimmung überwiegen. Die Gefahren der Videoüberwachung werden zudem– insbesondere vom BGH[111] – eindrucksvoll beschrieben.

Dabei sind beide Entscheidungen keineswegs eine Folge von Rechtsänderungen, die etwa durch den Geltungsbeginn der DSGVO bewirkt worden sein könnten. Allerdings könnte die allseits durch die Implementierung der DSGVO in Deutschland stark erhöhte generelle Aufmerksamkeit für Fragen des Datenschutzes und der Privatsphäre zu einer ebenfalls erhöhten Sensibilität der Gerichte beigetragen haben. Datenschutzbehörden und untere Gerichte sollten sich dadurch ermutigt fühlen, ihre Prüfmaßstäbe entsprechend zu schärfen.

---

108 Im Detail *Grabenschröer/Reuter*, in: Taeger/Gabel, DSGVO/BDSG, BDSG, § 4 Rn. 55.

109 BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883.

110 BVerwG, Urt. v. 27.3.2019 – 6 C 2.18, BeckRS 2019, 9874.

111 BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2886).

Der BGH hat zudem verstanden, dass die Videoüberwachung im öffentlichen Raum von einem überwiegend rechtlichen zu einem zunehmend technischen Thema geworden ist. Die Dashcam-Entscheidung des BGH war in dieser Hinsicht eine Landmarke (Privacy-by-design). Der Anwender muss sich vorhalten lassen, dass er die vorhandenen technischen Möglichkeiten, die Persönlichkeitsrechte Dritter zu schützen, nicht genutzt hat.[112] Mit Art. 25 DSGVO ist die Pflicht zum Einsatz von Technik, die die Rechte der Betroffenen möglichst schützt, auch geschriebenes Recht. Dabei ist der Stand der Technik zu berücksichtigen. Für den Anwender ist dies durchaus schwierig zu leisten, da es sich um ein dynamisches Konzept handelt. Der Verantwortliche muss sich laufend vergewissern, dass seine Maßnahmen noch dem aktuellen Stand entsprechen.[113]

In anderen Rechtsbereichen, insbesondere im Technischen Arbeitsschutz, kümmern sich rechtlich institutionalisierte Ausschüsse durch die Formulierung Technischer Regeln darum, die Praxis über den aktuellen Stand der Technik verbindlich zu informieren. Dies sollte Vorbild für den Datenschutz sein. Die Regeln sollten nicht vom Gesetzgeber selbst stammen, sondern auf einer zweiten, schneller reagierenden und fachlich versierten Regulierungsebene formuliert werden. Der Gesetzgeber muss aber dafür sorgen, dass diese Regeln sowohl Legitimität als auch rechtliche Verbindlichkeit bekommen, die über bloße Empfehlungen deutlich hinausgeht.[114] In Technischen Regeln könnte z.B. festgelegt werden, wie Bilddaten vor dem Zugriff Unbefugter zu sichern sind, welche Ereignisse Aufnahmen überhaupt erst automatisch auslösen oder wann und wie automatisch zu löschen ist. Die Privacy-by-design-Technik steht erst am Anfang der Entwicklung, wird aber sicher durch Künstliche Intelligenz vielfach befördert werden.

---

112 BGH, Urt. v. 15.5.2018 – VI ZR 233/17, NJW 2018, 2883 (2885), Rn. 25.

113 *Keber/Keppeler*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, DSGVO, Art. 25 Rn. 46.

114 Weitere Einzelheiten zu diesem Vorschlag in *Rose*, RDV 2019, S. 123 (131).

## Literatur

*Alexandrie, Gustav:* Surveillance cameras and crime: a review of randomized and natural experiments, Journal of Scandinavian Studies in Criminology and Crime Prevention 18, 2017, S. 210-222.

*Boehme-Neßler, Volker:* BilderRecht – Die Macht der Bilder und die Ohnmacht des Rechts, Berlin/Heidelberg 2010.

*Bornewasser, Manfred:* Evaluation der polizeilichen Videoüberwachung öffentlicher Straßen und Plätze im Land Brandenburg, Endbericht Juli 2005, in: Landtag Brandenburg – Drucksache 4/2347, 4.1.2006.

*Brandt, Daniela*: Wirkungen situativer Kriminalprävention - eine Evaluationsstudie zur Videoüberwachung in der Bundesrepublik Deutschland, Diplomarbeit Uni Bielefeld 2004, https://pub.uni-bielefeld.de/download/2306207/2306210 (zuletzt abgerufen am: 24.7.2019).

*Carver, Charles S./Scheier, Michael F.:* Attention and self-regulation: a control-theory approach to human behavior, New York et. al. 1981.

*Datenschutzkonferenz (DSK):* Videoüberwachung nach der Datenschutz-Grundverordnung, Kurzpapier Nr. 15, 8.1.2018, www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf (zuletzt abgerufen am: 24. 7.2019).

*Desoi, Monika:* Intelligente Videoüberwachung – rechtliche Bewertung und rechtsgemäße Gestaltung, Wiesbaden 2018.

*Düsseldorfer Kreis:* Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, 19.2.2014, www.lda.bayern.de/media/oh_videoueberwachung.pdf (zuletzt abgerufen am: 24.7.2019).

*Duval, Shelley/Wicklund, Robert A.:* A theory of objective self-awareness, New York 1972.

*Forsa Politik- und Sozialforschung GmbH*: Sicherheit in der Stadt – Ergebnisse einer repräsentativen Bevölkerungsbefragung, Berlin 2018.

*Geschke, Daniel/Klaßen, Anja/Quent, Matthias/Richter, Christoph:* #Hass im Netz: Der schleichende Angriff auf unsere Demokratie, Juni 2019, www.idz-jena.de/fileadmin/user_upload/_Hass_im_Netz_-_Der_schleichende_Angriff.pdf (zuletzt abgerufen am: 24.7.2019).

*Glancy, Dorothy J.:* The Invention of the Right to Privacy, Arizona Law Rev. 21, 1979, S. 1-39.

*Glaubitz, Christoffer/Kudlacek, Dominic/Neumann, Merten/Fleischer, Stephanie/Bliesener, Thomas*: Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gem. § 15a PolG NRW, KFN-Forschungsberichte No. 143, Hannover 2018.

*Gola, Peter (Hrsg.):* DS-GVO Kommentar, 2. Aufl., München 2018.

*Gola, Peter/Heckmann, Dirk (Hrsg.):* BDSG Kommentar, 13. Aufl., München 2019.

*Grages, Jan-Michael/Plath, Kai-Uwe:* Black Box statt Big Brother: Datenschutzkonforme Videoüberwachung unter BDSG und DSGVO, CR 2017, S. 791-797.

*Hurtz, Simon:* Kriminelle könnten Millionen Überwachungskameras übernehmen, SZ.de, 10.10.2018, www.sueddeutsche.de/digital/schwerwiegende-sicherheitsluecke-kriminelle-koennten-millionen-ueberwachungskameras-uebernehmen-1.4164949 (zuletzt abgerufen am: 24.7. 2019).

*Hempel, Leon/Alisch, Christian:* Evaluation der 24-Stunden-Videoaufzeichnung in U-Bahnstationen der Berliner Verkehrsbetriebe – Zwischenbericht, Berlin 2006, www.humanistische-union.de/nc/themen/datenschutz/videoueberwachung/videoueberwachung_details/back/videoueberwachung/article/videoueberwachung-in-den-u-bahnen-bringt-kein en-sicherheitsgewinn/ (zuletzt abgerufen am: 24.7.2019).

*Klar, Manuel:* Datenschutzrecht und die Visualisierung des öffentlichen Raums, Berlin 2012.

*Kudlacek, Dominic:* Akzeptanz von Videoüberwachung. Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen, Wiesbaden 2015.

*Kühl, Eike:* Superfood für Algorithmen – Soziale Netzwerke und Gesichtserkennung können eine gefährliche Kombination für die Privatsphäre sein, Zeit Online, 4.5.2016, www.zeit.de/digital/datenschutz/2016-05/findface-gesichtserkennung-republica-adam-harvey (zuletzt abgerufen am: 24.7.2019).

*Kühling, Jürgen/Buchner, Benedikt (Hrsg.):* Datenschutz-Grundverordnung/ BDSG Kommentar, 2. Aufl., München 2018.

*Lobe, Adrian:* Zeig mir dein Gesicht, Frankfurter Allgemeine, 28.5.2016, www.faz.net/aktuell/feuilleton/debatten/gesichtserkennungssysteme-gegen-terror-14255914.html (zuletzt abgerufen am: 24.7.2019).

*Lobinger, Katharina:* Visuelle Kommunikationsforschung. Medienbilder als Herausforderung für die Kommunikations- und Medienwissenschaft, Wiesbaden 2012.

*Piza, Eric L./Welsh, Brandon C./Farrington, David P./Thomas, Amanda L.:* CCTV and Crime Prevention. A New Systematic Review and Meta-Analysis, Stockholm 2018.

*Plath, Kai-Uwe (Hrsg.):* DSGVO/BDSG Kommentar, 3. Aufl., Köln 2018.

*Reinhold, Michael/Wortmann, Christoph:* Von der Gesichtsdetektion zur Emotionsanalyse, Marketing Review St. Gallen 2018, S. 888-894.

*Reuter, Wiebke:* Umgang mit sensiblen Daten bei allgemeiner Videoüberwachung. Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten, ZD 2018, S. 564-569.

*Rose, Edgar:* Erforderlichkeit und Interessengerechtigkeit der Videoüberwachung im öffentlichen Raum, RDV 2019, S. 123-131.

*Schneider, Jana/Schindler, Stephan:* Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten. Datenschutzrechtliche Anforderungen beim Erheben von Videodaten, ZD 2018, S. 463-469.

*Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.):* DS-GVO/BDSG Heidelberger Kommentar, Heidelberg 2018.

*Schwenke, Thomas:* Private Nutzung von Smartglasses im öffentlichen Raum, Edewecht 2016.

*Schwenke, Thomas:* Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, S. 823-827.

*Silvia, Paul J./Duval, T. Shelley:* Objective Self-Awareness Theory: Recent Progress and Enduring Problems, Personality and Social Psychology Review 5, 2001, S. 230-241.

*Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.):* Datenschutzrecht, Baden-Baden 2019.

*Taeger, Jürgen (Hrsg.):* Chancen und Risiken von Smart Cams im öffentlichen Raum, Baden-Baden 2017.

*Taeger, Jürgen/Gabel, Detlev (Hrsg.):* Kommentar DSGVO – BDSG, 3. Aufl. Frankfurt a. M. 2019.

*Todorov, Alexander*: Can We Read a Person's Character from Facial Images?, Scientific American, The discredited "science" of physiognomy is making an unfortunate comeback, 14.5.2018, https://blogs.scientifica merican.com/observations/can-we-read-a-persons-character-from-faci al-images/ (zuletzt abgerufen am: 24.7.2019).

*Willis, Janine/Todorov, Alexander:* Making Up Your Mind After a 100-Ms Exposure to a Face, Psychol Sci 17, 2006, S. 592-598.

*Wolff, Heinrich Amadeus/Brink, Stefan*: BeckOK Datenschutzrecht, 28. Ed., München 2019.

# ÖFFENTLICHE VIDEOÜBERWACHUNG AUS DER PERSPEKTIVE DES RUMÄNISCHEN RECHTS

Michaela Braun-Noviello - Rechtsanwältin

Rechtsanwaltskanzlei Braun-Noviello
info@europe-lawyers.eu

## 1 Zusammenfassung

Jeder Mensch im europäischen Raum hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass er dabei beobachtet oder gar aufgezeichnet wird. Jedoch, im Zusammenhang der Diskussionen zur Bekämpfung von Straftaten im öffentlichen Raum hat die Überwachung öffentlich zugänglicher Stellen viele Befürworter gewonnen. Diesen gegenüber stehen jedoch auch viele Verfechter, die die öffentliche Videoüberwachung im Hinblick auf die Persönlichkeitsrechte vehement ablehnen.

Für Befürworter der öffentlichen Videoüberwachung steht die eigene Sicherheit im Vordergrund. Sie vertreten die Meinung, dass durch die Anbringung von Überwachungskameras in den öffentlichen Räumen mit starkem Publikumsverkehr auf einer Seite das subjektive Sicherheitsgefühl gesteigert und zum anderen aber auch die objektive Wahrnehmung, dass Straftaten aufgezeichnet werden und somit aufgeklärt werden können, beruhigt werden.

In Rumänien war die gesellschaftliche Debatte pro und contra Videoüberwachung der öffentlichen Räume vor der Verabschiedung der Gesetze zur Umsetzung der EU-Datenschutz-Grundverordnung (DSGVO) eher als mäßig zu verzeichnen. Die politischen Unruhen der letzten Jahre haben die zivile Gesellschaft eventuell dermaßen beschäftigt, dass die öffentliche Debatte um die Sicherheit versus freie Persönlichkeitsentfaltung in den Schatten der politischen Kämpfe gerutscht ist.

Seit Wirksamwerden der DSGVO gelten für die Videoüberwachung der öffentlichen Räume auf der gesetzlichen Ebene strengere Voraussetzungen zum Schutz von personenbezogenen Daten.

## 2 Gesetzgebung

Mit dem 31.7.2018 ist in Rumänien das Gesetz 190/2018 zur Umsetzung der DSGVO in Kraft getreten. Dieses Gesetz ist im Wesentlichen eine unvollständige und teilweise ungenaue Übersetzung der DSGVO (speziell werden die Art. 6, 9, 37-39, 43, 83, 85, 87-89 wiederholt) und schafft somit

keine originären, an die konkreten, rumänischen Gegebenheiten angepassten Regelungen. Der dem nationalen Gesetzgeber durch die DSGVO eingeräumte Spielraum für die Implementierung von individuellen, nationalen Regelungen blieb fast ungenutzt. Spezifischere Regelungen enthält das rumänische Gesetz meistens im Bereich der Begriffsbestimmungen, so auch betreffend die Definitionen der öffentlichen Stellen und der darunter zählenden Entitäten, der nationalen Identifikationsnummer, des Berichtigungsplanes im Falle von Verstößen gegen die Schutzbestimmungen oder der Fristen zur Implementierung des Berichtigungsplans.

Bereits im Februar 2019 und somit nicht mal ein Jahr nach Inkrafttreten der DSGVO wurde dem rumänischen Parlament ein Entwurf zur Änderung des Art. 8 des Gesetzes 190/2018 vorgelegt, der die Verarbeitung von personenbezogenen Daten zu spezifischen Zwecken, genauer zu statistischen Zwecken, betrifft.

Durch das Inkrafttreten des Gesetzes 190/2018 sind die wichtigsten, vorherigen Gesetzte zum Schutz von personenbezogenen Daten gänzlich außer Kraft gesetzt worden, obwohl diese in ihrem wesentlichen Teil mit der DSGVO vereinbar waren und bestimmte Verarbeitungsmethoden von Personen bezogenen Daten - z.B. betreffend die öffentliche Videoüberwachung – genauer festlegten.

Somit wurde durch das Gesetz 190/2018 die Verordnung der Datenschutzaufsichtsbehörde Nr. 52/2012 gänzlich außer Kraft gesetzt. Diese Verordnung bildete die einzige genaue gesetzliche Grundlage für die Verarbeitung von personenbezogenen Daten durch Videoüberwachung im öffentlichen Bereich. Ergänzt wurden diese Bestimmungen durch das Gesetz Nr. 333/2003 über die Bewachung von Objekten, Gütern, Vermögen und über den Personenschutz und die methodischen Anwendungsnormen, das die allgemeine Pflicht zur Bewachung – und dadurch auch implizit Videoüberwachung als Bewachungsmethode – der öffentlichen Räumen vorsieht, wo besondere Vermögenswerte aufbewahrt werden oder sich Sachen vom besonderen Wert befinden.

Am 6.2.2019 trat das Gesetz Nr. 363/2018 über die Verarbeitung von personenbezogenen Daten durch Behörden zum Zwecke der Prävention und Aufklärung von Kriminalität in Kraft, wodurch die Umsetzung der Law-enforcement-Regelungen der DSGVO in das nationale Recht erfolgt ist.

Auf der Grundalge dieser Gesetze erließ die nationale Datenschutzaufsichtsbehörde (ANSPDCP) den Beschluss 174/2018, in dem die Verpflichtung der Verantwortlichen zur Durchführung von Risikoanalysen in bestimmten Fällen, darunter auch betreffend die öffentliche Videoüberwachung, vorgesehen wird.

### 2.1 Leitlinien für die Verarbeitung von personenbezogenen Daten im Allgemeinen

Die Gesetze 190 und 363 aus 2018 wiederholen die Mindestvoraussetzungen des Art. 6 DSGVO bei der Verarbeitung von personenbezogenen Daten, die rechtmäßig, nach Treu und Glauben, transparent, zweckbinden, richtig, minimal, begrenzt und vertraulich zu erfolgen hat. Zur Einhaltung dieser Grundsätze wird die Rechenschaftspflicht der Verantwortlichen begründet.

Genauere Bestimmungen zu der Verarbeitungsmethode durch Videoüberwachung betreffen lediglich die Videoüberwachung der Mitarbeiter durch den Arbeitgeber.

Art. 5 des Gesetzes 190/2018 ist die einzige Norm, die ausdrücklich die personenbezogene Datenverarbeitung durch Videoüberwachung regelt. Diese bezieht sich auf die Videoüberwachung am Arbeitsplatz, die nur als ultima ratio erfolgen darf. Der Verantwortliche muss den Nachweis erbringen können, das andere, weniger invasiven Methoden tatsächlich nicht zielführend waren.[1]

Die Speicherung der durch die Videoüberwachung verarbeiteten Daten kann maximal 30 Tage dauern. Die Gewährleistung der Rechte der Betroffenen (Informationsrecht, Auskunftsrecht, Veränderungs-, Übertragungs-, Löschungs-, Berichtigungs-, Widerspruchs-, Löschungsrecht) obliegt dem Arbeitgeber. Zur Realisierung dieser Verpflichtungen des Verantwortlichen (Arbeitgebers) und zur Sicherung der Verhältnis- und Zweckmäßigkeit ist ein Datenschutzbeauftragter zu bestellen.

Das Gesetz Nr. 363/2018 über den Schutz der natürlichen Personen bei der personenbezogenen Datenverarbeitung durch die zuständigen Behörden zwecks Vorbeugung, Aufdeckung, Ermittlung und Ahndung von Straftaten oder Vollstreckung von Strafen, Erziehungs- und Sicherungsmaßnahmen sowie betreffend deren freien Verkehr enthält erneut Definitionen und Begriffsbestimmungen, wonach personenbezogene Daten alle Informationen über eine identifizierte oder identifizierbare natürliche Person sind. Eine natürliche Person ist identifizierbar, wenn sie direkt oder indirekt durch Zuordnung zu einer Kennung (Identitätsnummer, anderem physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Merkmal) identifiziert werden kann.

---

[1] *Hogaș*, OFICIAL: în ce condiții vor putea firmele să își supravegeheze video angajații, din 31 iulie? Legestart 27/7/2018 (Nr. 7/2018), https://lege5.ro/Gratuit/gi4tanbygu4a/oficial-in-ce-conditii-vor-putea-firmele-sa-isi-supravegheze-video-angajatii-din-31-iulie (abgerufen am: 20.7.2019).

Die Verarbeitung von personenbezogenen Daten darf nur unter Einhaltung der Informations- und Auskunftsrechte der Betroffenen erfolgen, die durch die zwingend vorgesehene Bestellung eines Datenschutzbeauftragten zu gewährleisten ist.

Weiterhin werden die Verantwortlichen in bestimmten Fällen ausdrücklich zur Durchführung von Risikoanalysen und zur Dokumentierung aller Verarbeitungsvorgänge verpflichtet. Abhängig vom Stand der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie von den Ergebnissen der konkreten Risikoanalyse ist der Verantwortliche weiterhin verpflichtet, sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen. In den Verarbeitungsprozess sind die notwendigen Garantien zum Schutz der Rechte der betroffenen Personen aufzunehmen.

Ausnahmen von Auskunfts- und Informationsrechten sowie von Änderungs- und Löschungsrechten der Betroffenen sind im Wesentlichen im Gesetz 363/2018 geregelt und dienen der Aufklärung und Ahndung von Straftaten, der Strafvollstreckung oder der Sicherung eines normalen Verlaufs des Strafverfahrens.

Den Verantwortlichen obliegt die Meldung aller Verarbeitungsfehler- und -verstöße an die Aufsichtsbehörde und die Entwicklung eines Berichtigungsplanes, der unter Einhaltung einer Frist (90 Tage) implementiert werden soll. Über dessen Anwendung und Ergebnisse ist der Aufsichtsbehörde Bericht zu erstatten.

### 2.2 Die öffentliche Videoüberwachung

Die öffentliche Videoüberwachung ist eine Modalität der Verarbeitung von personenbezogenen Daten und stellt ein Eingriff in die Persönlichkeitsrechte dar, die im Art. 26 des rum. Grundgesetzes ihre Verankerung finden. Sie unterliegt den o.g. Gesetzen und darf nur unter Einhaltung der allgemeinen Grundsätze der Verarbeitung von personenbezogenen Daten eingesetzt werden. Sodann sind die Verantwortlichen (Behörden) zur Gewährleistung der Zweck-, Verhältnis- und Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten durch Videoüberwachung, der Grundsätze von Treu und Glauben, der Transparenz, der Datenminimierung, der Speicherbegrenzung und der Rechenschaftspflicht verpflichtet.

Die Videoüberwachung wird grundsätzlich zum Schutz von Personen und Eigentum, zur Sicherheit und Bewachung von Räumen des öffentlichen Interesses, zur Prävention von Kriminalität sowie zur Überwachung des öffentlichen Verkehrs eingesetzt.

Gem. Gesetz 333/2003 bedarf der Auftragsverarbeiter einer von Polizei auszustellenden Lizenz.

Nach Aufhebung des Beschlusses Nr. 52/2012 der Aufsichtsbehörde ANSPDCP gibt es keine nationale, ausdrückliche Gesetzesgrundlage für die öffentliche Videoüberwachung. Dennoch waren die genaueren Bestimmungen über die Durchführung der öffentlichen Videoüberwachung mit der DSGVO im Einklang, so dass sie weiterhin als Leitlinien dienen.

Demnach stellt die öffentliche Videoüberwachung eine Verarbeitung von personenbezogenen Daten auch dann vor, wenn die Aufnahmen keine Bilder der Betroffenen, aber andere Identifizierungsmerkmale festhalten (z.B. das amtliche Kfz-Kennzeichen).

Die öffentliche Videoüberwachung kann nur zu folgenden Zwecken durchgeführt werden:

a) Vorbeugung und Aufklärung von Straftaten;
b) Überwachung des öffentlichen Verkehrs und Feststellung von Verkehrsverstößen;
c) Schutz von Personen, Güter und Vermögen, von Immobilien und Einrichtungen des öffentlichen Gebrauchs und deren Umgebung;
d) Durchführung von Maßnahmen im öffentlichen Interesse oder Erfüllung der öffentlichen Aufgaben der Behörden;
e) Realisierung von geschützten Interessen des Verantwortlichen, wenn dabei die Grundrechte und Freiheiten der Betroffenen respektiert werden.

Die Videoüberwachung kann in den öffentlichen, dem Publikum zugänglichen Räumen, inklusive auf den Zugangswegen zu öffentlichen oder privaten Räumen unter Einhaltung folgenden Standards zum Schutz der allgemeinen Persönlichkeitsrechte der Betroffenen stattfinden:

a) Die Überwachungskameras werden an sichtbaren Stellen aufgehängt;
b) Videoüberwachungskameras dürfen nicht versteckt werden;
c) eine regelmäßige Risikoanalyse ist durchzuführen;
d) die Videoüberwachung ist in den Räumen, wo die Intimität von Personen vorrangig zu schützen ist, wie Umkleide-, Anprobe- Duschkabinen, Toiletten, ähnliche Räume, verboten.
e) die Betroffenen sind über die Videoüberwachung, deren Zweck und über den Verantwortlichen zu informieren;
f) Verhältnismäßigkeit der Dauer der Speicherung; Speicherbegrenzung;
g) Bestellung eines Datenschutzbeauftragten;
h) Dokumentierung der Vorgänge;
i) Meldepflicht bei Verstößen – Fristen;
j) Erstellung und Einführung von Berichtigungsplänen unter Einhaltung von Fristen;

k) Berichterstattung an die Aufsichtsbehörde – ANSPDCP

Ein vorgelagertes Hinweisschild - wie oben[2] – soll die wichtigsten Informationen wie Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten, Zweck und Rechtsgrundlage der Überwachung sowie Speicherdauer der Aufzeichnungen gut sichtbar bereitstellen. Weiterhin soll auf diesem Schild auf die Rechte der Betroffenen Person und auf den Empfänger der Daten hingewiesen werden.

Durch den Beschluss 174/2018 regelt die Aufsichtsbehörde bestimmte Verpflichtungen des Verantwortlichen näher.[3]

Art. 1:

Der Verantwortlicher/Auftragsverarbeiter ist zur Erstellung einer Risikoanalyse verpflichtet, siehe unter anderem:

c) bei der personenbezogenen Datenverarbeitung durch systematische Videoüberwachung von dem Publikum zugänglichen, öffentlichen Räumen: Einkaufszentren, Stadien, öffentlichen Plätzen und ähnliches;

d) bei der personenbezogenen Datenverarbeitung durch systematische Beobachtung des Verhaltens von schutzbedürftigen Personen (Minderjährigen) und Arbeitnehmern zum Zwecke von Marketing und Werbung.

---

[2] Verfügbar unter https://db.politiaromana.ro (zuletzt abgerufen am: 20.7.2019).

[3] ANSPDCP, Beschl. v. 18.10.2018, Az. 174/2018, https://www.dataprotection.ro/servlet/ViewDocument?id=1556 (abgerufen am: 20.7.2019).

Des Weiteren sollen die Ergebnisse der öffentlichen Videoüberwachung in einer bestimmten Zeitspanne im Verhältnis zu der Zweckmäßigkeit geprüft und bei der Erstellung der regelmäßigen Risikoanalyse berücksichtigt werden. Zwischen den gegenseitigen Interessen, wie etwa dem Schutz der Persönlichkeitsrechte und der Vorbeugung oder Aufdeckung von Kriminalität oder der Informations- und Meinungsfreiheit ist anhand von konkreten Ergebnissen eine Interessenabwägung vorzunehmen, die bei der Entscheidung über die Implementierung oder Fortsetzung einer Maßnahme die wesentliche Rolle spielen soll.

## 3 Praxis

Die Gesetze 190 und 363 aus 2018 sind ohne jegliche öffentliche Debatte verabschiedet worden. Lediglich einige Zeitungsberichte versuchten die Gesellschaft zu sensibilisieren, jedoch ohne jeglichen Aufschrei auszulösen. So wurde z.B. in der Zeitung „Libertatea" vom 10.6.2018 darüber berichtet, dass die Hauptstadt Bukarest mit 1709 Videoüberwachungskameras überwacht wird, wobei die meisten Verantwortlichen ihren gesetzlichen Informationspflichten nicht nachkommen.[4]

In einigen Regionalzeitungen sind auch Befragungen von Betroffenen – z.B. Taxifahrer – über Ihre Meinung zum Erfolg einer bestimmten Videoüberwachungsmaßnahme sporadisch zu lesen oder wird über die Kooperation zwischen den Verwaltungsbehörden als Verantwortliche in Bezug auf die öffentliche Videoüberwachung des Verkehrs und der Verkehrspolizei zwecks Feststellung der Identität von Verkehrssündern gewarnt.[5]

Betreffend die Entwicklung von Kriminalität in den videoüberwachten öffentlichen Räumen gibt es derzeit keine aktuellen, offiziellen Statistiken. Über die Zweckmäßigkeit der Videoüberwachung in bestimmten Fällen wird jedoch nicht nur auf der politischen Ebene heftig debattiert, wenn dadurch Gewaltstraftaten aufgeklärt werden können. So konnte im Oktober 2018 eine Frau verurteilt werden, die lediglich aufgrund einer Videoaufnahme einer Überwachungskamera an der Bukarester U-Bahn eindeutig als Täterin identifiziert werden konnte, die das Opfer auf den Gleisen schupste.[6] Die Mehrheit der Stimmen in der Gesellschaft war nach diesem sehr mediatisierten Vorfall der Meinung, dass die Videoüberwachung der

---

4 *Chilianu*, LIBERTATEA v. 10.6.2019, https://www.libertatea.ro/stiri/bucurestiul-este-monitorizat-cu-peste-1-700-de-camere-de-supraveghere-2286127 (abgerufen: 20.7.2019).

5 *Nechita*, radiocluj.ro v. 16.2.2018, http://www.radiocluj.ro/2018/02/16/camerele-din-traficul-clujean-vor-putea-fi-folosite-pentru-aplicarea-de-amenzi/ (abgerufen: 20.7.2019).

6 *Marin*, Gazeta de Sud v. 29.10.2018, https://www.gds.ro/Actualitate/2018-10-29/inchisoare-pe-viata-pentru-crima-de-la-metrou/ (abgerufen am: 20.7.2019).

öffentlichen Plätze mit viel Publikumsverkehr zum Zwecke der allgemeinen Sicherheit notwendig sei.

Derzeit wird im rumänischen Parlament über einen Gesetzesentwurf zur Einführung der Videoüberwachung in den Schulen, Kindergärten und anderen Bildungs- und Erziehungseinrichtungen zum Schutz der Kinder vor Gewalttaten diskutiert. Der Gesetzesentwurf sieht vor, dass Videoüberwachungsmaßnahmen mit der einfachen Mehrheit der Stimmen aller betroffenen Eltern bzw. Erziehungsberechtigten getroffen werden können. Wie die Rechte der anderen betroffenen Kinder, deren Eltern solchen Überwachungsmaßnahmen nicht zustimmen, zu garantieren sind, lässt der Gesetzesentwurf offen.[7]

Zu der bisherigen Aktivität der rumänischen Aufsichtsbehörde ist zu vermerken, dass laut dem offiziellen Bericht für die Zeitspanne vom 25.5.2018 bis zum 24.5.2019 folgende Ergebnisse zusammengefasst worden sind:

- es wurden 9439 Datenschutzbeauftragte gemeldet;
- 398 Meldungen über Verstöße und 5260 Beschwerden sind ergangen;
- 485 Prüfungen sind ex officio durchgeführt worden;
- 496 Prüfungen sind aufgrund von Beschwerden von Betroffenen erfolgt;
- 57 Berichtigungsmaßnahmen wurden angeordnet und 23 Verwarnungen wurden erteilt;
- das erste Bußgeld in Höhe von 130.000 EUR hat die Aufsichtsbehörde (ANSPDCP) am 27.6.2019 gegen Unikredit Bank SA wegen Verstoßes gegen den Art. 25 Abs. 1 DSGVO verhängt.[8]

Im Bereich der Videoüberwachung betreffen die Beschwerden eher den privaten Bereich, am häufigsten in den Fällen der Videoüberwachung von Wohneinheiten durch die Wohnungseigentümer, wobei die Überwachungskameras die Privatsphäre anderer Einwohner verletzen können.

Ähnlich gelagerte Rechtstreitigkeiten beschäftigen auch die Gerichte, die nun die Aufgabe haben, deutlich zu definieren, was im Zusammenhang mit der Videoüberwachung genau unter dem Begriff „öffentlichem Raum“ fällt. Die Entwicklung einer höchstrichterlichen Rechtsprechung ist noch abzuwarten.

---

[7] *Dobre*, legestart.ro v. 8.5.2019, https://legestart.ro/proiect-de-lege-pentru-dotarea-obligatorie-scolilor-cu-camere-video-de-supraveghere/ (abgerufen am: 20.7.2019).

[8] ANSPDCP, Pressemitteilung v. 4.7.2019, https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en (abgerufen am: 20.7.2019).

## Literatur

*Chilianu, Delia:* LIBERTATEA v. 10.6.2019, https://www.libertatea.ro/stiri/bucurestiul-este-monitorizat-cu-peste-1-700-de-camere-de-supraveghere-2286127 (zuletzt abgerufen am: 20.7.2019).

*Dobre, Traian:* legestart.ro v. 8.5.2019, https://legestart.ro/proiect-de-lege-pentru-dotarea-obligatorie-scolilor-cu-camere-video-de-supraveghere/.

*Hogaş, Elena:* OFICIAL: în ce condiţii vor putea firmele să îşi supravegeheze video angajaţii, din 31 iulie? Legestart 27/07/2018 (Nr. 7/2018), https://lege5.ro/Gratuit/gi4tanbygu4a/oficial-in-ce-conditii-vor-putea-firmele-sa-isi-supravegheze-video-angajatii-din-31-iulie (abgerufen am: 20.7.2019).

*Marin, Aldezir:* Gazeta de Sud v. 29.10.2018, https://www.gds.ro/Actualitate/2018-10-29/inchisoare-pe-viata-pentru-crima-de-la-metrou/ (abgerufen am: 20.7.2019).

*Nechita, Alina:* radiocluj.ro v. 16.2.2018, http://www.radiocluj.ro/2018/02/16/camerele-din-traficul-clujean-vor-putea-fi-folosite-pentru-aplicarea-de-amenzi/ (zuletzt abgerufen am: 20.7.2019).

# NEUE ENTWICKLUNGEN IM BESCHÄFTIGTENDATENSCHUTZRECHT

Prof. Dr. Prof. h.c. Jürgen Taeger

Direktor des Interdisziplinäres Zentrums für Recht der Informationsgesellschaft (ZRI), Carl von Ossietzky Universität Oldenburg
Vorsitzender der Deutschen Stiftung für Recht und Informatik (DGRI)
j.taeger@uol.de

## Zusammenfassung

Die EU-Datenschutz-Grundverordnung strebt die Vollharmonisierung des Datenschutzrechts in der Europäischen Union an. Sehr viele Öffnungsklauseln ermöglichen den Mitgliedstaaten, fachspezifische Datenschutzvorschriften beizubehalten oder neu zu schaffen. Dabei müssen die allgemeinen Grundsätze und im Wesentlichen die Pflichten der Verantwortlichen und die Rechte der Betroffenen aus der DSGVO berücksichtigt werden.

Deutschland hat u.a. von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht und mit § 26 BDSG Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten geschaffen, die weitgehend auf § 32 BDSG a.F. zurückgehen, um auf diesem Gebiet für Kontinuität zu sorgen. Außerdem wurden dabei einige Klarstellungen getroffen, so auch dahingehend, dass Einwilligungen im Beschäftigungsverhältnis grundsätzlich möglich sind (Erwägungsgrund 155 DSGVO; § 26 Abs. 2, Abs. 3 S. 2 BDSG) und sich eine Erlaubnis für die Verarbeitung von Beschäftigtendaten sich auch aus Kollektivvereinbarungen (ErwG 155 DSGVO; § 26 Abs. 1 und 4 BDSG i.V.m. Art. 88 Abs. 2 DSGVO) ergeben können.

Der folgende Beitrag stellt das Beschäftigtendatenschutzrecht im Überblick vor und geht auf ausgewählte Rechtsfragen näher ein.

## 1 Ziele der EU-Datenschutzreform

### 1.1 Räumlicher Anwendungsbereich und Marktortprinzip

Mit der Verabschiedung der Europäischen Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 gilt und gem. Art. 288 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) in allen EU-Mitgliedstaaten unmittelbar anzuwenden ist, verfolgt der Europäische Gesetzgeber zwei Ziele, die gleichrangig nebeneinander stehen. Art. 1 Abs. 1 DSGVO enthält die Gegenstandsbeschreibung der Verordnung, die natürliche Personen bei der Verarbeitung personenbezogener Daten schützen und zugleich den freien Verkehr personenbezogener Daten stärken soll. Diese Zielbestimmungen werden in den nachfolgenden Absätzen wieder aufgegriffen. So sollen gemäß Absatz 2 die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten durch die DSGVO gewährleistet werden. Im Grunde findet sich hier auch eine Definition des Begriffs ‚Datenschutz' wieder, weil

die DSGVO den Schutz ausschließlich der natürlichen Person vor Beeinträchtigung der verfassungsrechtlich verbürgten Persönlichkeitsrechte durch die Verarbeitung ihrer personenbezogenen Daten regelt, es also nicht um den Schutz von ‚Daten' geht, wie das Wort es suggerieren könnte. Gleichrangig soll die Verordnung aber auch der Gewährleistung des freien Verkehrs personenbezogener Daten dienen (Absatz 3). In der DSGVO finden sich sodann aber nur Vorschriften und Erwägungsgründe, die den Schutz natürlicher Personen vor den Gefährdungen durch die Datenverarbeitung verfolgen.[1]

Der räumliche Anwendungsbereich der DSGVO beschränkt sich gemäß Art. 3 Abs. 1 DSGVO zunächst „auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet". Mit Art. 3 Abs. 2 DSGVO i.V.m. Erwägungsgrund (ErwG) 23 gilt nun das Marktortprinzip. Damit wird der räumliche Anwendungsbereich faktisch auch auf Unternehmen ausgeweitet, die von außerhalb der EU betroffenen Personen auf dem europäischen Markt entgeltlich oder unentgeltlich Waren und Dienstleistungen in der EU anbieten (Art. 3 Abs. 2 lit. a DSGVO) oder die das Verhalten der betroffenen Personen beobachten (Art. 3 Abs. 2 lit. b DSGVO).

### 1.2 Vollharmonisierung und Öffnungsklauseln

Innerhalb der Europäischen Union sollte eine Harmonisierung des Datenschutzrechts erreicht werden, die unter der Datenschutz-Richtlinie (DSRL) nur partiell gelang. In der in allen Mitgliedstaaten unmittelbar anzuwendenden und Anwendungsvorrang vor nationalen Datenschutzvorschriften reklamierende Verordnung findet die Vollharmonisierung aber ihre Grenzen in den mehr als 70 Öffnungsklauseln. Sie sind häufig dem Umstand geschuldet, dass sich die Mitgliedstaaten in Detailfragen nicht auf einen Kompromiss einigen konnten und die Regelung den Mitgliedstaaten über eine Öffnungsklausel erlauben. Überspitzt formuliert könnte man von einer „Richtlinie im Gewand einer Verordnung"[2] und einem „Flickenteppich" sprechen, weil sich „die Bemühungen der EU, ein einheitliches, europäischen Datenschutzrecht für das 21. Jahrhundert zu schaffen, … nicht

[1] Siehe dazu ausführlich *Schmidt*, in: Taeger/Gabel, DSGVO BDSG, Art. 1 Rn. 1 ff.

[2] *Laue/Nink/Kremer*, Das neue Datenschutzrecht, § 1 Rn. 114; Ähnlich auch *Benecke/Wagner*, DVBl 2016, S. 600.

erfüllt“ hätten.[3] Der Kritik wird entgegengehalten, dass es sich bei Öffnungsklauseln „um eine für Rechtsakte der EU typische Regelungstechnik“ handele.[4]

Die Öffnungsklauseln enthalten entweder an die Mitgliedstaaten gerichtete Regelungsgebote, aufgrund derer sie bestehende nationale Datenschutzvorschriften anpassen oder auch schaffen müssen. Andere Öffnungsklauseln geben den Mitgliedstaaten aber auch Freiräume, fachspezifische Regelungen wie den Sozialdatenschutz beizubehalten oder den Datenschutz für bestimmte Anwendungsfälle zu spezifizieren und auszugestalten.[5]

Der deutsche Gesetzgeber hat hiervon Gebrauch gemacht und mit zwei Anpassungsgesetzen bestehende Gesetze mit Vorschriften zum Datenschutz an die Terminologie der Grundverordnung angepasst und im Rahmen der Öffnungsklauseln neue Vorschriften geschaffen. Von erheblicher Bedeutung ist die mit dem 1. Datenschutz-Anpassungs- und Umsetzungsgesetz (EU–DSAnpUG-EU)[6] erfolgte Aufhebung des Bundesdatenschutzgesetzes (BDSG a.F.) und die Verabschiedung eines neuen Bundesdatenschutzgesetzes (BDSG a.F.) zum 25.5.2018. Dieses neue BDSG wurde durch das am 26. November 2019 in Kraft getretene Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (EU – 2. DSAnpUG-EU),[7] das in 155 Artikeln in weiteren Gesetzen Anpassungen vornimmt, bereits wieder geändert. § 38 Abs. 1 Satz 1 BDSG bestimmt nun, dass Verantwortliche nichtöffentlicher Stellen und Auftragsverarbeiter erst dann einen Datenschutzbeauftragten zu bestellen haben, wenn 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind; vorher lag der Schwellenwert bei 10 Personen. Im Kontext mit dem Beschäftigtendatenschutz wird nun mit § 26 Abs. 2 S. 3 BDSG anerkannt, dass auch im Beschäftigungsverhältnis eine Einwilligung in elektronischer Form beispielsweise durch eine eMail oder durch Absendung eines elektronischen Webformulars mit einem die Einwilligung erklärenden Anklickens einer entsprechenden Checkbox wirksam erklärt werden kann.

---

3 *Reibach*, Nationales Datenschutzrecht – Die Deharmonisierung der DSGVO, in: Taeger, Rechtsfragen digitaler Transformationen, S. 131 (140); Kritisch auch *Pohl*, PinG 2017, S. 85.

4 *Albrecht/Janson*, CR 2016, S. 500.

5 Ausführlich zu Umfang und Wirkung der Öffnungsklauseln *Reibach* (Fn. 3); Vgl. auch *Piltz*, K&R 2016, S. 557; und *Roßnagel*, DuD 2017, S. 277.

6 BGBl I 2017, 2097.

7 BGBl I 2019, 1626.

### 1.3 Öffnungsklausel für den Beschäftigtendatenschutz

Aufgrund der Öffnungsklausel des Art. 88 Abs. 1 DSGVO dürfen die Mitgliedstaaten „spezifische Vorschriften zur Gewährleistung der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigtenkontext“ beibehalten oder verabschieden.[8] Ausdrücklich stellt nun die DSGVO in Art. 88 Abs. 1 Satz 1 DSGVO klar, dass auch Kollektivvereinbarungen solche Vorschriften zum Beschäftigtendatenschutz enthalten können.

Von dieser mit Art. 88 DSGVO geschaffenen Möglichkeit machte der Gesetzgeber mit § 26 BDSG Gebrauch.[9] In § 26 BDSG finden sich Erlaubnistatbestände für die Verarbeitung personenbezogener Daten von Beschäftigten im Sinne von § 26 Abs. 8 BDSG. Danach dürfen „personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist“ (§ 26 Abs. 1 S. 1 BDSG).

Diese Vorschriften sind auf alle Beschäftigten öffentlicher Stellen des Bundes und nichtöffentlicher Stellen anzuwenden. Sie würden auch in den Bundesländern für die Beschäftigten landesunmittelbarer öffentlicher Stellen gelten, soweit diese keine eigenen Landesdatenschutzgesetze geschaffen haben. Weil das aber inzwischen mit an die DSGVO angepassten Inhalten geschehen ist, findet der § 26 BDSG auf Beschäftigte landesunmittelbarer Stellen[10] keine Anwendung. Dort lassen sich allerdings keine mit § 26 BDSG vergleichbaren Vorschriften finden, sodass die Verarbeitung dieser Beschäftigtendaten nach Art. 6 Abs. 1 UAbs. 1 DSGVO zu richten hat, sofern nicht im Einzelfall sehr spezifische Regelungen getroffen wurden.[11]

---

[8] Ausführlich *Höhne*, Auswirkungen der unionsrechtlichen Öffnungsklausel nach Art. 88 DSGVO auf den Beschäftigtendatenschutz nach deutschem Recht; Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes vor Inkrafttreten der DSGVO 2016 *Taeger/Rose*, BB 2016, S. 819.

[9] Siehe zu den bereichsspezifischen Regelungen des Beschäftigtendatenschutzes in den Ländern *Gola*, ZD 2018, S. 448.

[10] Stellen des Landes, der Kommunen und der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Personen und Stellen außerhalb des öffentlichen Bereichs, soweit ihnen Aufgaben der öffentlichen Verwaltung übertragen sind.

[11] Siehe etwa § 12 NDSG.

Bevor die Erlaubnis zur Verarbeitung von Beschäftigtendaten durch § 26 BDSG oder durch Art. 6 Abs. 1 UAbs. 1 DSGVO näher betrachtet werden, sind die allgemeinen, auch bei der Verarbeitung von Beschäftigtendaten aufgrund einer Erlaubnis nach § 26 BDSG zu beachtenden Grundsätze aus Art. 5 DSGVO zu betrachten.

## 2 Grundsätze und Verhaltenspflichten der DSGVO

### 2.1 Verbot mit Erlaubnisvorbehalt

Der Europäische Gesetzgeber hat seinen grundrechtliche Schutzpflichten aus Art. 7 und 8 GrCh (Kombinationsgrundrecht)[12] und speziell Art. 7 Abs. 2 GrCh entsprechend in der DSGVO das Verbot der Datenverarbeitung mit Erlaubnisvorbehalt festgeschrieben.[13] Verantwortliche müssen für die Verarbeitung eine Erlaubnis haben, die sich aus einem Gesetz Erlaubnis oder einer Einwilligung ergeben kann. Ohne eine solche Erlaubnis ist die Verarbeitung rechtswidrig; sie kann mit einem Bußgeld gem. Art. 83 Abs. 5 DSGVO geahndet werden.[14] Werden besondere Kategorien personenbezogener Daten oder Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet, so sind die speziellen Anforderungen der Art. 9 und 10 DSGVO zu beachten.

Ergibt sich bei einem ersten Prüfschritt danach die Rechtmäßigkeit einer Verarbeitung, so hat der Verantwortliche im Fall der Übermittlung der personenbezogenen Daten in ein Drittland in einem zweiten Schritt zusätzlich zu prüfen, ob die besonderen Rechtmäßigkeitsvoraussetzungen der Art. 44 ff. DSGVO gegeben sind. Das kann aus mehreren Gründen der Fall sein. So kann von Europäischen Kommission ein Angemessenheitsbeschluss ergangen sein, nach dem im Zielland ein angemessenes Schutzniveau vorhanden ist (Art. 45 DSGVO), weswegen die Übermittlung in das Drittland unbedenklich erscheint. Eine Drittlandsübermittlung könnte auch zulässig sein, wenn der Verantwortliche oder der Auftragsverarbeiter gem. Art. 46 DSGVO „geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe

[12] BVerfG, Beschl. v. 6.11.2019 – 1 BvR 276/17 (Recht auf Vergessen II): „Die Gewährleistungen der Art. 7 und Art. 8 GRCh sind dabei eng aufeinander bezogen. Jedenfalls soweit es um die Verarbeitung personenbezogener Daten geht, bilden diese beiden Grundrechte eine einheitliche Schutzverbürgung“.

[13] Näher zur Bedeutung dieses Verbotes *Taeger*, in: Taeger/Gabel, DSGVO BDSG, Art. 6 Rn. 3 ff.

[14] Siehe dazu das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 14.10.2019 vorgelegte Konzept der DSK zur Bußgeldzumessung in Verfahren gegen Unternehmen, https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.

zur Verfügung stehen". Solche könnten sich nach dem Katalog in Art. 46 Abs. 2 DSGVO u.a. aus verbindlichen internen Datenschutzvorschriften (binding corporate rules, Art. 47 DSGVO), genehmigten branchenspezifischen Verhaltensregeln und genehmigten Zertifizierungen (Art. 46 Abs. 2 lit. e und f) oder aus der Anwendung der EU-Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c und lit. d DSGVO ergeben.

### 2.2 Bußgeldbewehrte Grundsätze

Der Verantwortliche hat bei der (erlaubten) Verarbeitung allerdings auch die allgemeinen Grundsätze zu beachten, die sich aus Art. 5 Abs. 1 DSGVO ergeben,[15] und muss die Einhaltung dieser Grundsätze nachweisen, also Rechenschaft ablegen können (Accountability). Auch die Missachtung dieser Pflichten kann durch ein Bußgeld sanktioniert werden, das „wirksam, verhältnismäßig und abschreckend sein" soll (Art. 83 Abs. 1; 84 Abs. 1 Satz 2 DSGVO). Bei Verstößen gegen Art. 6 und Art. 5 DSGVO droht eine Geldbuße „von bis zu 20 000 000 € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs […], je nachdem, welcher der Beträge höher ist" (Art. 83 Abs. 5 DSGVO).

Der erste Grundsatz verlangt, dass die Daten rechtmäßig und unter Beachtung des Grundsatzes von Treu und Glauben[16] und transparent verarbeitet werden. Die Informations- und Auskunftspflichten aus Art. 13, 14, 15 DSGVO nehmen auf das Transparenzgebot Bezug.

Daten dürfen nicht auf Vorrat zu noch unbekannten Zwecken erhoben werden. Der Zweck muss eindeutig benannt werden können. Mit der Erhebung eines personenbezogenen Datums können auch mehrere Zwecke verfolgt werden. Es muss also bei Aufnahme der Verarbeitung festgehalten werden, zu welchem bestimmten Zweck sie erfolgt, zumal auch die Betroffenen darüber zu unterrichten sind (Art. 13 Abs. 1 lit. c bzw. Art. 14 Abs. 1 lit. c DSGVO). Trotz der Bindung der Erhebung an einen bestimmten Zweck ist unter Beachtung der Kriterien aus Art. 6 Abs. 4 DSGVO[17] eine zweckändernde Weiterverarbeitung zulässig.

Der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO bedeutet letztlich nicht, dass Daten nur in einem absolut minimalen Umfang

[15] Ausführlich zu den Verarbeitungsgrundsätzen *Voigt*, in: Taeger/Gabel, DSGVO BDSG, Art. 5 Rn. 8 ff.

[16] Siehe zur Auslegung dieses nur schwer greifbaren Merkmals *Voigt*, in: Taeger/Gabel, DSGVO BDSG, Art. 5 Rn. 13 ff.

[17] Siehe zur Kritik an dieser Regelung über die zweckändernde Weiterverarbeitung *Taeger*, in: Taeger/Gabel, DSGVO BDSG, Art. 6 Rn. 138.

gespeichert werden dürfen; die Praxis zeigt, dass in vielen Fällen dieses Minimum schwer festlegbar und kontrollieren ist. Von Bedeutung ist in diesem Zusammenhang aber Art. 25 DSGVO, der den Datenschutz durch Technikgestaltung (data protection/privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) behandelt und sich im Wortlaut auch unmittelbar auf den Grundsatz der Datenminimierung bezieht. Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen und durch Voreinstellung nur personenbezogene Daten zu verarbeiten, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Der Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO) erfordert, dass Daten sachlich korrekt und aktuell sind. Stimmen die Daten mit der Realität nicht überein und sind somit unrichtig, sind sie – soweit keine Ausnahmegründe gem. Art. 17 Abs. 3 DSGVO vorliegen – vom Verantwortlichen zu löschen oder ihre Verarbeitung ist einzuschränken (Art. 18 DSGVO/§ 35 BDSG). Mit dieser Verpflichtung korrespondiert das Recht der betroffenen Person, dass unrichtige Daten unverzüglich berichtigt werden (Art. 16 DSGVO).[18] Eine Löschung ist vorzunehmen, wenn einer der in Art. 17 Abs. 1 DSGVO aufgeführten Gründe vorliegt,[19] insbesondere dann, wenn die Verarbeitung der Daten nicht mehr erforderlich ist oder sie unrechtmäßig erfolgt.[20]

Die von Art. 5 Abs. 1 lit. e DSGVO geforderte Speicherbegrenzung erfordert eine kontinuierliche Überprüfung durch den Verantwortlichen, ob die personenbezogenen Daten noch gespeichert werden müssen bzw. der Personenbezug aufrecht erhalten werden muss.[21] Es ist folglich bei Aufnahme der Verarbeitung auch ein Löschkonzept vorzusehen.

### 2.3 Allgemeine Geltung der Grundsätze

Diese Grundsätze sind nicht nur dann zu beachten, wenn die Verarbeitung aufgrund eines Erlaubnistatbestands aus Art. 6 oder Art. 9 DSGVO folgt. Sie gelten als unabdingbares Recht – mit der nicht unwesentlichen Möglichkeit der sich aus Art. 23 DSGVO ergebenden Beschränkung – auch

[18] Zu den Voraussetzungen des Berichtigungsrechts *Meents/Hinzpeter*, in: Taeger/Gabel, DSGVO BDSG, Art. 16 Rn. 8 ff.; zu den Grenzen dieses Anspruchs *Voigt*, in: Taeger/Gabel, DSGVO BDSG, Art. 5 Rn. 32.

[19] Zu den Problemen bei der Umsetzung *Keppeler/Berning*, ZD 2017, S. 314; Vgl. zu Löschpflichten auch *Dovas*, ITRB 2017, S. 186; speziell in der Personalverwaltung *Haußmann/Karwatzki/Ernst*, DB 2018, S. 2697; und *Grimm/Kühne*, ArbRB 2018, S. 144.

[20] Näher dazu *Meents/Hinzpeter*, in: Taeger/Gabel, DSGVO BDSG, Art. 17 Rn. 27 ff.

[21] Vgl. zu den Anforderungen VG Karlsruhe, Urt. v. 6.7.2017 – 10 K 7698/16, m. Anm. *Ehmann*, ZD 2017, S. 543; Siehe auch *Moos*, Update Datenschutz, in: Taeger, Rechtsfragen digitaler Transformationen, S. 259 (264, 266).

dann, wenn sich die Erlaubnis aus einer fachspezifischen Vorschrift wie dem § 26 BDSG hinsichtlich der Beschäftigtendaten ergibt. Entsprechendes gilt auch für die vom Verantwortlichen zu beachtenden Verhaltenspflichten, soweit sie nicht ausnahmsweise wegen des Umfangs der Datenverarbeitung und der dann als geringer eingeschätzten Risiken ausgenommen sind, namentlich für die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, die Vornahme der Rechtsfolgenabschätzung, die Bestellung eines Datenschutzbeauftragten (intern/extern), die Beachtung der Informationspflichten, die vertragliche Regelung der Auftragsverarbeitung und die Gewährleistung der Betroffenenrechte. Die Rahmenbedingungen der Verarbeitung machen den Standard des Europäischen Datenschutzrechts aus, innerhalb dessen Spezifizierungen einschließlich fachspezifischer Erlaubnisnormen durch nationales Recht im Rahmen der Öffnungsklauseln zulässig sind.

## 3 Verarbeitung von Beschäftigtendaten

Die DSGVO enthält keine spezifischen Vorschriften zum Beschäftigtendatenschutz und insbesondere keinen besonderen Erlaubnistatbestand zur Verarbeitung von Daten für Zwecke des Beschäftigungsverhältnisses. Nur in Art. 9 Abs. 2 lit. b DSGVO wird als Ausnahme des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten die Verarbeitung in den Fällen erlaubt, in denen sie erforderlich ist, „damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht“.

### 3.1 Öffnungsklausel für nationale Rechtsvorschriften und Kollektivvereinbarungen zum Beschäftigungsverhältnis

Die Öffnungsklausel des Art. 88 DSGVO (Datenverarbeitung im Beschäftigungskontext) in Verbindung mit ErwG 155 erlaubt den Mitgliedstaaten, „durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags, … des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigen-

tums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses" vorzusehen. Der deutsche Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht und für die Verarbeitung von Beschäftigtendaten besondere Erlaubnistatbestände in § 26 BDSG geschaffen. Im Beschäftigtendatenschutzrecht gibt es innerhalb der EU folglich keine Vollharmonisierung.

Bei der Auslegung des Begriffs ‚Rechtsvorschrift' in der deutschen Übersetzung der DSGVO ist zu beachten, dass es in der französischen Fassung „par la loi" und in der englischen Fassung „by law" heißt, so dass neben Gesetzen im formellen Sinn auch das Gewohnheitsrecht und die richterliche Rechtsfortbildung eingeschlossen sind.[22]

Der Begriff des Beschäftigten ist sehr weit zu fassen. Nach der Definition des § 26 Abs. 8 BDSG gehören dazu die Arbeitnehmer des Verantwortlichen, aber auch die bei ihm tätigen Leiarbeitnehmer, die zugleich Beschäftigte des Entleihers' sind, Personen in der Berufsausbildung, Rehabilitanden, Freiwillige aus Freiwilligendiensten, Arbeitnehmerähnliche Personen wie die Heimarbeiter und Crowdworker, Beamte, Richter und Soldaten sowie die Bewerber und ausgeschiedene Personen.

Zu beachten ist die nationale Sonderregelung, dass § 26 Abs. 7 BDSG den sachlichen Anwendungsbereich gegenüber Art. 1 Abs. 1 DSGVO erweitert. Während die Anwendbarkeit der DSGVO davon abhängt, dass personenbezogene Daten ganz oder teilweise automatisiert oder in Dateisystemen als einer strukturierten Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind (Art. 4 Nr. 6 DSGVO), verarbeitet werden, fallen auch (unstrukturierte) Akten mit darin enthaltenen Beschäftigtendaten in den Anwendungsbereich des § 26 BDSG.

Nach der Gesetzesbegründung führt § 26 BDSG die spezialgesetzliche Regelung des § 32 BDSG a. F. fort.[23] Dementsprechend wird die Kontinuität der bisherigen Rechtsprechung zum Arbeitnehmerdatenschutz erwartet.[24] Der Gesetzgeber behält sich ausweislich der Gesetzesbegründung vor, das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von

[22] *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 3.

[23] BT-Drs. 18/11325, S. 96 f.

[24] *Laue*, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 9 Rn. 8.

Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken entsprechend der bisherigen Rechtsprechung gesondert zu regeln.

### 3.2 Erlaubnistatbestände des Beschäftigtendatenschutzes

Nach § 26 Abs. 1 Satz 1 BDSG ist die Verarbeitung von Beschäftigtendaten, die für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, zu den hier aufgeführten Zwecken erlaubt.

#### 3.2.1 Verarbeitung im Bewerbungsverfahren

Bei einer Bewerbung auf eine ausgeschriebene Stelle dürfen die personenbezogenen Daten der Bewerber, die nach § 26 Abs. 8 DSGVO Beschäftigte im Sinne des Gesetzes sind, vom Verantwortlichen aufgrund der gesetzlichen Erlaubnis aus § 26 Abs. 1 Satz 1 BDSG verarbeitet werden, sofern sie für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses benötigt werden.[25] Es muss ein berechtigtes Interesse des Arbeitgebers an den Bewerberdaten vorhanden sein.[26] Das ist der Fall, soweit dadurch eine Beurteilung der Eignung für die vorgesehene Tätigkeit möglich wird, etwa durch Angaben über die fachlichen und persönlichen Fähigkeiten, Kenntnisse und Erfahrungen.[27] Diese Anforderung gilt auch für diejenigen Daten, die der Arbeitgeber vor der Einstellungsentscheidung in beruflichen Zwecken dienenden Social Media-Plattformen oder bei Dritten einholt. Damit nicht vereinbar wäre es, wenn ein Arbeitgeber Bewerbern einen Standardfragebogen vorlegen würde, mit dem alle Daten abgefragt werden, die für jeden im Unternehmen in Betracht kommenden Arbeitsplatz benötigte Daten abfragt, auch wenn viele Informationen für die zu besetzende Stelle nicht benötigt werden. Ein solcher Fragebogen darf nicht verwendet werden.

Auch mit Inkrafttreten des § 26 Abs. 1 BDSG ist die Rechtsprechung zum Fragerecht des Arbeitgebers wegen der Kontinuität der Vorschrift nach § 32 BDSG a.F. uneingeschränkt zu beachten.

Umstritten ist wegen des Verbots des Profiling gemäß Art. 22 DSGVO, ob bei einem eRecruiting-Verfahren eine automatisierte Auswahl aus den Bewerbungen vorgenommen werden darf. Zwar heißt es in Art. 22 Abs. 2 DSGVO, dass das Verbot des Profiling nicht gilt, wenn es für den Abschluss eines Vertrags erforderlich ist. Daraus wird man aber nur ableiten können,

---

[25] Dazu näher *Bettinghausen/Wiemers*, DB 2018, S. 1277; *Grimm/Kühne*, ArbB 2018, S. 245; *Hafenmayer*, DB 2019, S. 2354.

[26] Siehe *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 30.

[27] Instruktiv die Begründung zum Gesetzesentwurf zum Beschäftigtendatenschutz aus 2013, RegE § 32 Abs. 1 S. 2, BT-Drs. 17/4230; Ausführlich hierzu *Gola*, Handbuch Beschäftigtendatenschutz, S. 157 ff.

dass in Verfahren mit großen Anzahl von Bewerbungen eine Vorauswahl getroffen und das automatisierte Auswahlverfahren dabei unterstützend eingesetzt werden darf.

Nach Abschluss des Einstellungsverfahrens dürfen die Daten zu dem Zweck gespeichert bleiben, soweit die Verarbeitung nach Art. 17 Abs. 3 lit. e DSGVO zur Verteidigung von Rechtsansprüchen des Arbeitgebers erforderlich ist. Anerkannt ist, dass dies solange zulässig ist, wie mit einem Anspruch auf Entschädigungszahlung nach § 15 AGG wegen Diskriminierung eines abgelehnten Bewerbers gerechnet werden kann, was wegen § 61b Abs. 1 ArbGG eine Speicherdauer von drei Monaten nach der ausgesprochenen Ablehnung bedeutet.

Sollen Daten abgelehnter Bewerber in einem Datenpool oder in einer Bewerberdatenbank weiter gespeichert bleiben, ist dies nur mit einer längsten ein Jahr wirkenden Einwilligung (Art. 6, 7 DSGVO) möglich. Die Einwilligung kann aber darüber hinaus zeitlich erneuert werden.

### 3.2.2 Verarbeitung zur Durchführung des Beschäftigungsverhältnisses

Die Beschäftigtendatenverarbeitung ist zur Durchführung des Beschäftigtenverhältnisses zulässig. Auch diese Alternative hat ihren Ursprung in § 32 Abs. 1 BDSG a.F. Soweit auf eine im Beschäftigungskontext stehende Verarbeitung verwiesen wird, ist darunter jede Datenverarbeitung zu verstehen, die einen Zusammenhang mit dem Arbeitsverhältnis aufweist.

Der Arbeitgeber ist auf eine große Vielfalt an Daten über den Beschäftigten angewiesen. Das beginnt bei den Daten, die zur Erfüllung der arbeitsvertraglichen Pflichten des Arbeitgebers, etwa zur Berechnung und Auszahlung des Lohnes bzw. Gehaltes erforderlich sind. Sodann müssen Daten über die Arbeitserfüllung des Beschäftigten einschließlich der Fehlzeiten verarbeiten werden. Der Arbeitgeber ist durch zahlreiche gesetzliche Vorschriften verpflichtet, Informationen über die Beschäftigten zu erheben, bereit zu halten und an verschiedene Stellen zu übermitteln. Dabei steht der § 26 Abs. 1 Satz 1 DSGVO in Konkurrenz zu der Erlaubnisvorschrift aus Art. 6 Abs. 1 Satz 1 lit. c DSGVO in Verbindung mit der jeweiligen Gesetzesnorm, die zu einer solchen Verarbeitung verpflichtet. Schon der Wortlaut des § 26 Abs. 1 Satz 1 2. Alt. BDSG gibt eine Vorstellung von der Weite der Anwendungsfälle, die durch diese Erlaubnis abgedeckt sind.[28]

### 3.2.3 Verarbeitung bei Beendigung des Beschäftigungsverhältnisses

Bei allen im Rahmen der aus welchem Grund auch immer (Aufhebung, Kündigung, Ruhestand, Tod) erfolgenden Beendigung des Beschäftigungs-

[28] Siehe die Beispiele bei *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 39 ff.

verhältnisses dürfen die damit im Zusammenhang stehenden erforderlichen Verarbeitungen von Beschäftigtendaten aufgrund der Erlaubnis aus § 26 Abs. 1 Satz 1 3. Alt. BDSG vorgenommen werden.

Die Verarbeitung von Daten von verstorbenen Beschäftigten wird nicht durch das BDSG geregelt, wie überhaupt Daten verstorbener Personen nicht in den Anwendungsbereich des Datenschutzrechts fallen. ErwG 27 weist darauf hin, dass die Mitgliedstaaten die Möglichkeit haben, Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorzusehen. Davon hat Deutschland bislang keinen Gebrauch gemacht. Grenzen der Verarbeitung dieser Daten ergeben sich aus dem Schutz des postmortalen Persönlichkeitsrechts.

### 3.3 Einwilligung als Erlaubnis der Verarbeitung von Beschäftigtendaten

§ 26 Abs. 2 BDSG bestätigt zunächst mittelbar, dass die Einwilligung im Beschäftigungsverhältnis ein Erlaubnistatbestand sein kann. Der Erlaubnistatbestand der Einwilligung folgt allerdings direkt aus Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO in Verbindung mit Art. 4 Nr. 11 und Art. 7 DSGVO.

Vor dem Inkrafttreten des BDSG wurden Zweifel geäußert, ob Beschäftigte innerhalb des Subordinationsverhältnisses mit seinem strukturellen Ungleichgewicht überhaupt wirksam in die Verarbeitung ihrer Daten durch den Arbeitgeber einwilligen können, wenn keine gesetzliche Erlaubnis vorliegt.[29] Teilweise wurde dies gänzlich ausgeschlossen, weil Beschäftigte im Arbeitsverhältnis niemals frei von Zwang sein könnten.[30]

Der § 26 Abs. 2 Satz 1 BDSG stellt nun klar, dass sich im Beschäftigungsverhältnis ein Arbeitgeber doch auf eine Einwilligung als wirksame Erlaubnis stützen kann. Das gilt nach § 26 Abs. 3 Satz 2 BDSG auch für besondere Kategorien personenbezogener Daten des Beschäftigten. In solchen Fällen ist die einwilligende Person ausdrücklich darauf hinzuweisen, dass sich die Einwilligung auf diese besonders schutzwürdigen Daten bezieht. Vor Abgabe der Einwilligungserklärung muss der Zweck der Verarbeitung der Beschäftigtendaten transparent sein.

In jedem Fall muss für den Verantwortlichen die Gewissheit bestehen, dass die Einwilligungserklärung freiwillig erfolgt. Situationen, in denen das beispielsweise der Fall ist, werden in § 26 Abs. 2 Satz 2 BDSG aufgezählt. Bei der Prüfung des Merkmals der ‚Freiwilligkeit' sind die aus Art. 4 Nr. 11 und Art. 7 DSGVO folgenden Bedingungen und ergänzend die besonderen Bedingungen des § 26 Abs. 2 BDSG zu beachten. Schon aus Art. 4 Nr. 11

[29] Siehe näher zur Einwilligungsmöglichkeit unter dem BDSG a.F. *Taeger*, in: Taeger/Gabel, BDSG, 2. Aufl., § 4a Rn. 63 ff.; *Taeger*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl., Art. 7 Rn. 96 ff.; *Taeger/Rose*, BB 2016, S. 819 (822).

[30] Neben anderen *Simitis*, AuR 2001, S. 429 (431).

DSGVO folgt, dass die Einwilligung eine "freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung [ist], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist". Freiwilligkeit setzt auch und besonders im Beschäftigungsverhältnis voraus, dass sie ohne jeden Zwang oder Druck erfolgte. Der Beschäftigte muss davon ausgehen können, dass eine Verweigerung der Einwilligung oder einen Widerruf keine Nachteile zur Folge hat. Ob im Abhängigkeitsverhältnis eine freie Entscheidung möglich ist, muss im Einzelfall sorgfältig geprüft werden.

Die Einwilligungserklärung kann seit Inkrafttreten des 2. DSAnpUG-EU am 26.11.2019 aufgrund der Änderung in § 26 Abs. 2 Satz 3 BDSG nun auch durch eine eindeutige Erklärung in elektronischer Form erfolgen.

### 3.4 Erforderlichkeitsprüfung

Die Zulässigkeit der Verarbeitung von Beschäftigtendaten auf der Grundlage des § 26 Abs. 1 Satz 1 BDSG setzt voraus, dass die Verarbeitung für den festgelegten Zweck auch erforderlich ist.[31] Es ist demnach eine Verhältnismäßigkeitsprüfung vorzunehmen. Die Verarbeitung muss zu der von der Rechtsprechung gebilligten Zweckerreichung förderlich sein (Geeignetheit). Es dürfen keine für den Arbeitgeber zumutbaren weniger eingreifenden Mittel verfügbar sein (Erforderlichkeit i.e.S.). Die Interessen des Arbeitgebers müssen mit denen der Beschäftigten abgewogen worden sein (Angemessenheit). Die Erforderlichkeitsprüfung ist streng durchzuführen, wenn gegen einen Beschäftigten Überwachungsmaßnahmen erfolgen sollen. Die Missachtung der Erforderlichkeitsprüfung oder die fehlerhaft zum Nachteil des Beschäftigten durchgeführte Erforderlichkeitsprüfung führt zu einem Beweisverwertungsverbot, wenn durch die unverhältnismäßige Verarbeitung den Beschäftigten belastende Informationen erlangt wurden,[32] weil die Erforderlichkeit eine materiell-rechtliche Zulässigkeitsvoraussetzung ist.

### 3.5 Kollektivvereinbarungen

§ 26 Abs. 1 S. 1 und Abs. 4 BDSG wiederholen (überflüssigerweise) die Vorschrift des Art. 88 Abs. 2 DSGVO, wonach die Verarbeitung von Beschäftigtendaten auch aufgrund einer die Verarbeitung regelnden Kollektivvereinbarung, also eines Tarifvertrages und Betriebs-, Dienst- oder

[31] *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 25.

[32] BAG, Urt. v. 20.6.2013 – 2 AZR 546/12, RDV 2014, 103, Rn. 28 (noch zu § 32 BDSG a.F.); BAG, Urt. v. 27.7.2017 – 2 AZR 681/16, RDV 2017, 291.

Sprechervereinbarung zulässig ist.[33] Schon die Öffnungsklausel nennt die Kollektivvereinbarung als spezifische Vorschrift, aus der sich Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten ergeben können, wobei nach Art. 88 Abs. 2 DSGVO angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person zu berücksichtigen sind. Die Schutzstandards der DSGVO sind, wenn eine Kollektivvereinbarung, typerweise eine Betriebsvereinbarung, eine Erlaubnis enthält, einzuhalten (§ 26 Abs. 5 BDSG).

### 3.6 Beschäftigtendatenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 DSGVO

Soweit ein Arbeitgeber personenbezogene Daten von Beschäftigten verarbeitet, ohne dass es einen Beschäftigungskontext gibt, so ist neben der Einwilligung auch eine Erlaubnis aus Art. 6 Abs. 1 UAbs. 1 DSGVO denkbar.[34] So kann es einen Vertrag mit einem Beschäftigten über die Nutzung eines unternehmenseigenen Parkplatzes geben, einen Mietvertrag über eine Werkswohnung oder eines Ferienappartements oder eine Vereinbarung über die Teilnahme an einem betrieblichen Altersvorsorgeprogramm. Dann wäre Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO für die Verarbeitung der dafür erforderlichen Daten die richtige Erlaubnisgrundlage.

Müssen Beschäftigtendaten zur Erfüllung gesetzlicher Pflichten verarbeitet werden, was nur mittelbar im Beschäftigungskontext steht, so ist Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i.V.m. dem Fachrecht die Erlaubnisgrundlage. Dazu gehören sozial- und steuerrechtliche Pflichten oder der umstrittene Terrorlistenabgleich.[35]

Denkbar ist auch, dass die Verarbeitung von Beschäftigtendaten, insbesondere von Fach- und Führungskräften im Rahmen einer Due Diligence notwendig wird und eine Aufhebung des Personenbezugs mangels wirksamer Anonymisierung nicht möglich ist. In diesem Fall ergäbe sich die Erlaubnis aus Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Wird die Verarbeitung hierauf gestützt, sind die Betroffenen unter Hinweis auf ihr Widerspruchsrecht zu informieren; das mit dem Widerspruch geltend gemachte Interesse am Unterlassen der Datenverarbeitung muss gegenüber dem Interesse des Arbeitgebers überwiegen.

---

[33] Vgl. dazu *Körner*, NZA 2019, S. 1389.

[34] *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 11; *Maschmann*, in: Kühling/Buchner, DSGVO BDSG, Art. 88 Rn. 21; *Laue*, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 9 Rn. 4 f.; *Düwell/Brink*, NZA 2017, S. 1081.

[35] *Gola*, Handbuch Beschäftigtendatenschutz, S. 337, Rn. 1479.

# 4 Einzelfälle

## 4.1 Betriebsrat als Verantwortlicher

Kontrovers wird die Frage diskutiert, ob der Betriebsrat selbst Verantwortlicher[36] ist oder Teil der verantwortlichen Stelle.[37] Wäre er selbst Verantwortlicher für die von ihm verarbeiteten personenbezogenen Daten, so müsste er nach der Legaldefinition des Art. 4 Nr. 7 DSGVO „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten" entscheiden. Über die Zwecke entscheidet der Betriebsrat schon deswegen nicht, weil ihm die Datenverarbeitung „nur im Rahmen der ihm zugewiesenen Aufgaben",[38] insbesondere des Betriebsverfassungsgesetzes, erlaubt ist und der Verordnungsgeber keine Legitimation habe, in die spezifischen betriebsverfassungsrechtlichen Strukturen einzugreifen.

Vor allem aber handelt der Betriebsrat nur im Rahmen der durch das Betriebsverfassungsgesetz zugewiesenen Aufgaben. Möglich ist, dass dem Betriebsrat durch Kollektivvereinbarungen weitergehende Befugnisse eingeräumt werden, die ihm zusätzliche Überwachungsaufgaben zuweisen, zu deren Zweckerfüllung er Beschäftigtendaten verarbeiten darf. Darüber hinaus kann der Betriebsrat keine weitere Zwecke von sich aus festlegen. Über Sachmittel für die IT-Ausstattung und damit die Datenverarbeitung entscheidet der Betriebsrat nicht frei, auch wenn er zur Erfüllung seiner Aufgaben einen Anspruch gegenüber dem Arbeitgeber auf die erforderliche Ausstattung hat.

Wäre der Betriebsbrat selbst Verantwortlicher, dann dürfte auch der betriebliche Datenschutzbeauftragte des Arbeitgebers die Einhaltung des Datenschutzes beim Betriebsrat nicht kontrollieren, der dann allein für die Einhaltung der Grundsätze und Pflichten aus der DSGVO und dem BDSG verantwortlich wäre. Er wäre zudem – neben dem Arbeitgeber für dessen Sphäre – Adressat der Betroffenenrechte und der Transparenzpflichten. Bei

---

[36] Vertreten von LAG Sachsen-Anhalt, Beschl. v. 18.12.2018 – 4 TaBV 19/17 –, RDV 2019, 141, m. zust. Anm. *Brors/Weingärtner*, DB 2019, S. 1156; *Kurzböck/Weinbeck*, BB 2018, S. 1652; *Kleinebrink*, DB 2018, S. 2566; *Brink/Joos*, jurisPR-ArbR 33/2019 Anm. 1; *Grimm*, in: Tschöpe, Arbeitsrechts-Handbuch, Beschäftigtendatenschutz und Social Media, Rn. 124; und ohne jegliche Begründung *Kramer*, in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, C. I. Rn. 47.

[37] So Hess. LAG, Beschl. v. 10.12.2018 – 16 TaBV 130/18, RDV 2019, 143, m. abl. Anm. *Möllenkamp*, NZA-RR 2019, S. 198; *Stück*, ZD 2019, S. 256; *Bott/Vogel*, BB 2019, S. 2100; *Bonanni/Niklas*, ArbRB 2018, 371; *Schmidl/Wolff*, AuA 2018, S. 696; *Brams/Möhle*, ZD 2018, S. 570-573; *Gola*, in: Gola, DS-GVO, Art. 4 Rn. 56; *Heuschmid*, SR 2019, S. 1; *Middel*, ArbuR 2018, S. 411; *Däubler-Gmelin*, CuA 8/2019, S. 8.

[38] *Körner*, Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis, S. 58.

Verstößen gegen Datenschutzvorschriften wäre er zu sanktionieren, obwohl ihm Mittel nicht zur Verfügung stehen, aus denen die Bußgelder gezahlt werden könnten.

Nach alledem überzeugt die Ansicht, dass der Betriebsrat nicht Verantwortlicher im datenschutzrechtlichen Sinn ist, sondern weiterhin mit der Rechtsprechung des BAG[39] als Teil der verantwortlichen Stelle anzusehen ist.

### 4.2 Videoüberwachung am Arbeitsplatz

Wird im Unternehmen eine Videoüberwachungsanlage eingesetzt, mit der das Verhalten von Beschäftigten zum Schutz der unternehmerischen Handlungsfreiheit und des Eigentums des Arbeitgebers überwacht wird, kollidiert dies mit dem Allgemeinen Persönlichkeitsrecht des Beschäftigten, der sich nicht einer dauerhaften Überwachung ausgesetzt sehen will. Sie ist deshalb nur zulässig, wenn und soweit eine gesetzliche Vorschrift die Überwachung erlaubt. Eine solche Erlaubnis ergibt sich wegen des spezifischen Einsatzzwecks weder aus Art. 6 Abs. 1 UAbs. 1 DSGVO noch aus § 4 BDSG, bei der der überwachte Raum zudem öffentlich zugänglich sein müsste, sondern aus § 26 BDSG als der spezielleren Vorschrift.

Das Bundesarbeitsgericht wendet zu Recht die speziellere Vorschrift des Beschäftigtendatenschutzes (jetzt: § 26 Abs. 1 Satz 1 DSGVO) an[40] und nicht die Regelung zur Videoüberwachung des öffentlichen Raumes an (jetzt: § 4 BDSG). Auch hier ist der Verhältnismäßigkeitsgrundsatz streng zu beachten. Danach wird eine anlasslose Dauerüberwachung zur Prävention schon wegen des dadurch erzeugten Überwachungsdrucks[41] regelmäßig unzulässig sein.[42]

Eine anders zu bewertende Situation wird vorliegen, wenn es zu dokumentierende tatsächliche Anhaltspunkte dafür gibt, dass eine beschäftigte Person eine Straftat begangen hat. Für diese Fälle sieht § 26 Abs. 1 Satz 2 BDSG ausdrücklich vor, dass Daten – auch durch eine Videoüberwachung – erhoben werden dürfen. Das Gesetz spricht ausdrücklich vom Anhaltspunkt für eine ‚Straftat'. Die Vorschrift legitimiert also keine repressive Überwachung zur Aufklärung von Pflichtverletzungen oder Ordnungswidrigkeiten.[43] Eine solche Maßnahme könnte in engen Grenzen nur nach § 26

[39] BAG, Beschl. v. 14.1.2014 – 1 ABR 54/12, RDV 2014, 277, Rn. 28.

[40] Anders noch das BAG, Urt. v. 21.6.2012 – 2 AZR 153/11, RDV 2012, 297.

[41] BAG, Urt. v. 27.3.2003 – 2 AZR 51/02, RDV 2003, 293, Rn. 25; BAG, Urt. v. 21.6.2012 – 2 AZR 153/11, RDV 2012, 297, Rn. 30; BAG, Urt. v. 23.8.2018 – 2 AZR 133/18, RDV 2018, 333, Rn. 43; BAG, Urt. v. 28.3.2019 – 8 AZR 421/17, NZA 2019, 12, Rn. 39.

[42] Siehe dazu *Grimm*, jM 2016, S. 17.

[43] Ebenso *Maschmann*, in: Kühling/Buchner, DS-GVO BDSG, § 26 Rn. 58 m.w.N.

Abs. 1 Satz 1 BDSG zulässig sein.[44] Das Bundesarbeitsgericht dehnt diesen Begriff allerdings weit aus und versteht darunter auch schwere Vertragspflichtverletzungen.[45]

Der Verhältnismäßigkeitsgrundsatz ist auch hier zu beachten, weshalb die Vorschrift hervorhebt, dass die Verarbeitung nur zulässig ist, wenn „die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind".

Wurden diese Anforderungen nicht beachtet, so war die Verarbeitung von Anfang an rechtswidrig. Die so erlangten Daten werden in einem Gerichtsverfahren nicht verwertet werden dürfen.[46] Eine offene Videoüberwachung in einem öffentlich zugänglichen Kassenraum, die aus präventiven Erwägungen eingerichtet wurde, kann nach § 26 Abs. 1 Satz 1 BDSG zulässig sein, wenn kein übermäßiger Überwachungsdruck besteht. Ist diese offene Videoüberwachung in einem öffentlich zugänglichen Raum, die auch nach § 4 BDSG zu beurteilen ist, anfänglich rechtmäßig, so ist doch umstritten, ob die Aufnahmen von Beschäftigten auch dann gegen sie verwendet werden dürfen, wenn sie nicht zeitnah gelöscht und die Aufnahmen dann bei Entstehen eines Tatverdachts noch lange nach der Aufnahme herangezogen werden.[47]

Neben der Entscheidung, welche Vorschrift für eine Videoüberwachung in öffentlich zugänglichen Räumen, die auch dort Beschäftigte mit erfasst, anzuwenden ist, steht eine andere wesentliche Frage im Raum, die nach der Speicherdauer von Videoaufzeichnungen. Schon aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) folgt, dass die Videoaufzeichnungen nicht etwa deshalb dauerhaft aufbewahrt werden dürfen, weil sie unter Umständen einmal benötigt würden. Eine unbegrenzte Speicherdauer ist zudem unverhältnismäßig. Kritisch wird bemerkt, dass durch diese Sichtweise die Grenzen einer präventiven Überwachung gemäß § 26 Abs. 1 Satz 1 BDSG zu jener einer repressiven Überwachung nach Satz 2 verschwimmen würden.[48]

Das BAG sah in der Entscheidung vom 23.8.2018 allerdings kein Verwertungsverbot im Kündigungsschutzprozess, weil eine ursprünglich zulässige

---

[44] *Zöll*, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 47.

[45] BAG, Urt. v. 27.7.2017 – 2 AZR 681/16, RDV 2017, 291 (Keylogger).

[46] Dazu ausführlich *Eufinger*, DB 2017, S. 1266 (1268).

[47] BAG, Urt. v. 23.8.2018 – 2 AZR 133/18, RDV 2018, 333.

[48] *Brink/Joos*, jurisPR-ArbR 38/2019 Anm. 1; Ähnlich auch *Neugebauer*, DB 2019, S. 2359.

Videoüberwachung nicht durch Zeitablauf unverhältnismäßig wird, solange die Rechtsverfolgung durch den Arbeitgeber noch möglich sei. Das Gericht hält den Verstoß gegen datenschutzrechtlich unzulässig lange Speicherdauer (hier: 6 Monate) für nicht so gravierend, dass dies bei einer Abwägung zu einem Beweisverwertungsverbot führen müsse. Damit bestätigt das BAG seine häufig im Widerspruch zu den Landesarbeitsgerichten stehende Rechtsprechung, nach der aus dem Verfahrensrecht kein generelles Verbot der Verwertung von angebotenen Beweisen gebe, sondern es im Einzelfall einer Abwägung bedürfe.[49]

Eine solche Sichtweise, die das Erfordernis einer zeitlichen Begrenzung der Speicherung negiert, könnte als Aufruf an Arbeitgeber missverstanden werden, Videoaufzeichnungen auf Vorrat zu speichern. Diese Entscheidung ist daher zu Recht auf Ablehnung gestoßen.[50] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat dementsprechend darauf hingewiesen, dass die BAG-Rechtsprechung ihn nicht daran hindere, Arbeitgeber wegen der dauerhaften und damit rechtswidrigen Speicherung des Videomaterials wegen eines Datenschutzverstoßes zu sanktionieren.

### 4.3 Namentliche Unterrichtung des Betriebsrats über Schwangerschaften

Das Bundesarbeitsgericht entschied, dass § 26 Abs. 3 S. 1 BDSG die Erlaubnisgrundlage für die Übermittlung der Namen der schwangeren Arbeitnehmerin durch den Arbeitgeber ist, weil der Betriebsrat nach § 80 Abs. 2 S. 1 BetrVG einen entsprechenden Auskunftsanspruch habe, wenn dem Arbeitgeber gemäß § 15 Abs. 1 MuSchG eine Schwangerschaft anzeigt.[51] Ein Widerspruch der Schwangeren kann diese datenschutzrechtliche Zulässigkeit nicht beseitigen; die Unterrichtung ist auch nicht von der Einwilligung der Schwangeren abhängig. Allerdings hat der Betriebsrat bei einer Verarbeitung besonderer Kategorien personenbezogener Daten, wozu die Information über eine Schwangerschaft gehört, angemessene und spezifische Schutzmaßnahmen gemäß § 22 Abs. 2 BDSG zu treffen. Ist das nicht der Fall, überwiegen schutzwürdige Interessen der Betroffenen mit der Folge, dass die Information des Betriebsrats datenschutzrechtlich unzulässig ist.

---

[49] Ausführlich dazu *Fuhlrott/Schröder*, NZA 2017, S. 278.

[50] *Brink/Schwab*, jurisPR-ArbR 6/2019 Anm. 5; *Tiedemann*, ZD 2019, S. 230. A.A. *Thüsing*, EWiR 2018, S. 633.

[51] BAG, Beschl. v. 9.4.2019 – 1 ABR 51/17, RDV 2019, 2810, m. zust. Anm. *Lelley/Bruck*, EWiR 2019, S. 569; *Hitzelberger-Kijima*, DB 2019, S. 2248; m. krit. Anm. *von Roetteken*, jurisPR-ArbR 37/2019 Anm. 7.

Eine entsprechende Bewertung, so das BAG,[52] muss auch der Anspruch des Betriebsrats auf Benennung derjenigen Arbeitnehmer erfahren, die die Voraussetzungen für die Durchführung des betrieblichen Eingliederungsmanagements erfüllen.

Der Betriebsrat hat aufgrund des ihm durch § 80 Abs. 1 BetrVG zugewiesenen Überwachungsrechts auch das Recht der Einsichtnahme in nichtanonymisierte Gehaltslisten.[53] Datenschutzrechtlich ist dies eine Verarbeitung in Form der Nutzung nach § 26 Abs. 1 Satz 1 BDSG.[54]

## 5 Fazit

Die Regulierung des Beschäftigtendatenschutzes ist ein Beleg dafür, dass die Vollharmonisierung des Datenschutzrechts in der Europäischen Union nur unzulänglich gelungen ist. Die mit der Öffnungsklausel des Art. 88 DSGVO geschaffene spezifische Regulierung des Beschäftigtendatenschutzes hat in Deutschland für Kontinuität gesorgt, so dass die zu § 32 BDSG a.F. ergangene Rechtsprechung in vielen Fragen des Beschäftigtendatenschutzes herangezogen werden kann. Aber längst sind auch durch die Rechtsprechung nicht alle Fragen geklärt.[55] So bleibt das Verhältnis der Videoüberwachung nach § 4 BDSG zu der präventiven Videoüberwachung in öffentlich zugänglichen Räumen nach § 26 Abs. 1 Satz 1 BDSG und diese Videoüberwachung wiederum zur Videoüberwachung zur Aufklärung von Straftaten nach § 26 Abs. 1 Satz 2 BDSG weiterhin ungeklärt. Auch ist kaum nachvollziehbar, weshalb die nach Satz 2 zulässige Videoüberwachung zur Aufklärung von Straftaten nach der Rechtsprechung des BAG auch bei einem Verdacht einer schweren Vertragspflichtverletzung herangezogen werden kann. Absatz 2 entfaltet keine Sperrwirkung bei der Aufklärung von Ordnungswidrigkeiten oder Pflichtverletzungen; vielmehr können verhältnismäßige Maßnahmen zur Aufklärung in diesen Fällen auf § 26 Abs. 1 Satz 1 BDSG oder Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt werden.[56] Hier wird wohl ein anderer Erlaubnistatbestand herangezogen

[52] BAG, Beschl. v. 7.2.2012 – 1 ABR 46/10, RDV 2012, 193, noch zum BDSG a.F. Anderer Ansicht ist die Nds. LfDI, die eine Mitteilung nur in anonymisierter Form als zulässig ansieht, LfDI Nds., Typische Fälle im Beschäftigtendatenschutz, 2018, https://lfd.nie dersachsen.de/download/127627/Typische_Fallbeispiele_im_Beschaeftigtendatenschutz_Stand_November_2018_pdf.

[53] BAG, Beschl. v. 7.5.2019 – 1 ABR 53/17, ZD 2019, 571; Kritisch dazu *Weller*, BB 2019, S. 3008.

[54] LAG Nds., Beschl. v. 22.10.2018 – 12 TaBV 23/18, ZD 2019, 178, m. Anm. *Stück*, ZD 2019, S. 180.

[55] Siehe auch *Gräber/Nolden*, in: Paal/Pauly, DS-GVO BDSG, § 26 Rn. 57 ff.

[56] *Dzida/Grau*, NZA 2017, S. 1515; *Zöll*, in: Taeger/Gabel, DSGVO BDSG, 2019, § 26 Rn. 47.

werden müssen, der vor dem EuGH bestehen kann. Es wird im Datenschutzrecht und insbesondere im Beschäftigtendatenschutzrecht noch einige Zeit dauern, bis der Europäische Datenschutzausschuss (EDSA) und der EuGH für mehr Rechtssicherheit gesorgt haben werden.

## Literatur

*Albrecht, Jan Philipp/Janson, Nils J.:* Datenschutz und Meinungsfreiheit nach der Datenschutzgrundverordnung, CR 2016, S. 500-509.

*Benecke, Alexander/Wagner, Julian:* Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG, DVBl 2016, S. 600-608.

*Bettinghausen, Mina/Wiemers, Matthias:* Bewerberdatenschutz nach neuem Datenschutzrecht, DB 2018, S. 1277-1283.

*Bonanni, Andrea/Niklas, Lisa-Marie:* Ist der Betriebsrat „Verantwortlicher" im Sinn der DSGVO?, ArbRB 2018, S. 371-374.

*Bott, Ingo/Vogel, Jan-Patrick:* Sanktionen gegen Betriebsrat und Betriebsratsmitglieder nach der DSGVO?, BB 2019, S. 2100-2102.

*Brams, Isabelle/Möhle, Jan-Peter:* Die Stellung des Betriebsrats unter der DSGVO, ZD 2018, S. 570-573.

*Brink, Stefan/Schwab, Sabrina:* Zur Speicherfrist einer offenen Videoüberwachung, jurisPR-ArbR 6/2019 Anm. 5.

*Brink, Stefan/Joos, Daniel:* Einsichtsrecht des Betriebsrats in nicht anonymisierte Bruttolohn- und Gehaltslisten und ohne Überwachung seitens des Arbeitgebers, jurisPR-ArbR 33/2019 Anm. 1.

*Brink, Stefan/Joos, Daniel:* Verwertungsverbote bei der Videoüberwachung von Beschäftigten, jurisPR-ArbR 38/2019 Anm. 1.

*Däubler-Gmelin, Herta:* Rechte und Pflichten im Datenschutz, CuA 8/2019, S. 8-16.

*Dovas, Maria-Urania:* Die Pflicht zur Löschung von Daten: Änderungen durch die DSG-VO und Umsetzung im Unternehmen, ITRB 2017, S. 186-191.

*Düwell, Franz Josef/Brink, Stefan:* Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung – Viele Änderungen und wenig Neues, NZA 2017, S. 1081-1085.

*Dzida, Boris/Grau, Timon:* Datenschutzrechtliche Rechtfertigung von Maßnahmen zur Aufklärung von Pflichtverstößen unterhalb der Strafbarkeitsschwelle, NZA 2017, S. 1515-1519.

*Eufinger, Alexander:* Arbeitsrechtliche Beweisverwertungsverbote und unternehmensinterne Untersuchungen, DB 2017, S 1266-1271.

*Fuhlrott, Michael/Schröder, Thomas:* Beschäftigtendatenschutz und arbeitsgerichtliche Beweisverwertung, NZA 2017, S. 278-283.

*Gola, Peter:* Der Beschäftigtendatenschutz in den novellierten Landesdatenschutzgesetzen, ZD 2018, S. 448-452.

*Gola, Peter (Hrsg.):* DS-GVO Kommentar, 2. Aufl., München 2018.

*Gola, Peter:* Handbuch Beschäftigtendatenschutz, 8. Aufl., Frechen 2019.

*Grimm, Detlef:* Überwachung im Arbeitsverhältnis, jM 2016, S. 17-27.

*Grimm, Detlef/Kühne, Jonas:* Löschkonzepte nach der DSGVO – Alle Aufbewahrungspflichten und -rechte sowie Löschfristen bei Beschäftigtendaten im Überblick, ArbRB 2018, S. 144-149.

*Grimm, Detlef/Kühne, Jonas:* Datenschutz und Datenschutzerklärung für Bewerber, ArbB 2018, S. 245-249.

*Hafenmayer, Angelika:* Bewerbungsunterlagen: Einsichtnahmerechte einzelner Personengruppen, DB 2019, S. 2354-2357.

*Haußmann, Katrin/Karwatzki, Constance/Ernst, Sebastian:* Datenschutzrechtliche Löschfristen in der Personalverwaltung, DB 2018, S. 2697-2702.

*Heuschmid, Johannes:* Datenschutzgrundverordnung und Betriebsverfassung, SR 2019, S. 1-11.

*Höhne, Katharina:* Auswirkungen der unionsrechtlichen Öffnungsklausel nach Art. 88 DSGVO auf den Beschäftigtendatenschutz nach deutschem Recht, Hamburg 2019.

*Keppeler, Lutz Martin/Berning, Wilhelm:* Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten, ZD 2017, S. 314-319.

*Kleinebrink, Wolfgang:* Arbeitgeber und Betriebsrat als „Verantwortliche“ im neuen Datenschutzrecht?, DB 2018, S. 2566-2571.

*Körner, Marita:* Die Auswirkungen der Datenschutz-Grundverordnung (DSGVO) in der betrieblichen Praxis, Frankfurt am Main 2019.

*Körner, Marita:* Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung des DS-GVO, NZA 2019, S. 1389-1395.

*Kühling, Jürgen/Buchner, Benedikt (Hrsg.):* Datenschutz-Grundverordnung/ BDSG Kommentar, 2. Aufl., München 2018.

*Kurzböck, Christoph/Weinbeck, Kathrin:* DSGVO-Verstöße im Betriebsratsbüro – wer haftet?, BB 2018, S. 1652-1655.

*Laue, Philip/Nink, Judith/Kremer, Sascha:* Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

*Laue, Philip/Kremer, Sascha:* Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Baden-Baden 2019.

*Middel, Lukas:* Beschäftigtendatenschutz im Lichte der DSGVO und unter Berücksichtigung des BDSG (neu), ArbuR 2018, S. 411.

*Moos, Flemming:* Update Datenschutz, in: Jürgen Taeger, Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 259-271.

*Paal, Boris P./Pauly, Daniel A.:* DS-GVO BDSG, 2. Aufl., Baden-Baden 2018.

*Piltz, Carlo:* Die Datenschutz-Grundverordnung, K&R 2016, S. 557-567.

*Plath, Kai-Uwe (Hrsg.):* DSGVO/BDSG Kommentar, 3. Aufl., Köln 2018.

*Pohl, Dirk:* Durchsetzungsdefizite der DSGVO?, PinG 2017, S. 85-91.

*Reibach, Boris:* Nationales Datenschutzrecht – Die Deharmonisierung der DSGVO, in: Jürgen Taeger (Hrsg.), Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht 2018, S. 131-141.

*Roßnagel, Alexander:* Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, DuD 2017, S. 277-281.

*Schmidl, Michael/Wolff, Alexander:* „Verantwortlicher" i.S.d. DSGVO?, AuA 2018, S. 696-699.

*Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.):* DS-GVO/BDSG Heidelberger Kommentar, Heidelberg 2018.

*Simitis, Spiros:* Arbeitnehmerdatenschutzgesetz – Realistische Erwartung oder Lippenbekenntnis?, AuR 2001, S. 429-433.

*Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.):* Datenschutzrecht, Baden-Baden 2019.

*Stück, Volker:* Betriebsrat oder Geheimrat?, ZD 2019, S. 256-261.

*Taeger, Jürgen/Rose, Edgar:* Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes, BB 2016, S. 819-831.

*Taeger, Jürgen/Gabel, Detlev (Hrsg.):* Kommentar DSGVO – BDSG, 3. Aufl., Frankfurt a. M. 2019.

*Tiedemann, Jens:* Offene Videoüberwachung – Verdachtskündigung – Beweisverwertungsverbot, ZD 2019, S. 230-231.

*Thüsing, Gregor:* Zur gerichtlichen Verwertung von Bildsequenzen aus einer zulässigen offenen Videoüberwachung im Verfahren gegen den Arbeitnehmer, EWiR 2018, S. 633-634.

*Tschöpe, Ulrich:* Arbeitsrecht Handbuch, 11. Aufl., Köln 2019.

*Weller, Bernd:* Betriebsrat kann Einblick in namensscharfe Bruttogehaltslisten der Mitarbeiter verlangen, BB 2019, S. 3008.

*Weth, Stephan/Herberger, Maximilian/Wächter, Michael/Sorge, Christoph (Hrsg.):* Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., München 2019.

*Wolff, Heinrich Amadeus/Brink, Stefan*: BeckOK Datenschutzrecht, 28. Ed., München 2019.

*Wybitul, Tim:* Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, S. 413-419.

# DATENVERARBEITUNG IM BESCHÄFTIGUNGSVERHÄLTNIS ZUR AUFDECKUNG VON STRAFTATEN

Rechtsanwalt Radu Hodis-Mayer

Raab & Kollegen, Fürth
rh@rk-rechtsanwaelte.de

## Einführung

Die Mitgliedstaaten haben über die Eröffnungsklausel in Art. 88 DS-GVO die Möglichkeit, durch *„Rechtsvorschriften oder durch Kollektivvereinbarungen“* die Datenverarbeitung im Beschäftigungskontext näher zu regeln.[1] Hiervon hat der deutsche Gesetzgeber mit § 26 BDSG Gebrauch gemacht. Die Rechtsprechung hat sich in der Vergangenheit mit der Zulässigkeit der Datenverarbeitung im Beschäftigungsverhältnis nach Maßgabe des § 32 BDSG a.F. auseinandergesetzt. Auch wenn in der Literatur die Übertragung der von der Rechtsprechung zu einer verdeckten Videoüberwachung entwickelten Grundsätze auf § 26 BDSG teilweise abgelehnt wird, sind die Regelungen des § 32 BDSG a.F. letztendlich *„weitgehend wortgleich in § 26 überführt worden“*.[2] Es besteht jedenfalls die Möglichkeit, dass diese Grundsätze auch künftig, wenn auch nur teilweise, in der Rechtsprechung Beachtung finden. Vor diesem Hintergrund untersucht dieser Aufsatz anhand einer Entscheidung des BAG zu BDSG a.F. diese Grundsätze.

## 1 Sachverhalt

In seinem Urteil vom 20.10.2016 – 2 AZR 395/15 hat sich das BAG mit der Frage befasst, inwiefern personenbezogene Daten im Beschäftigungsverhältnis zur Aufdeckung von Straftaten erhoben, verarbeitet oder benutzt und unter welchen Bedingungen die sich daraus ergebenden Erkenntnisse in einem Kündigungsschutzverfahren verwendet werden können.

In einem Ersatzteillager der Beklagten, einem Kfz-Vertragshändler, wurden Inventurdifferenzen festgestellt. Bis zu diesem Zeitpunkt durften die Mitarbeiter eigenhändig Teile aus dem Lager entnehmen und falls diese doch nicht benötigt wurden, zurückbringen.

Mit Hilfe eines Aushangs wurden diese Differenzen im Betrieb bekannt gemacht. Die bisherige Handhabe wurde dahingehend geändert, dass den

---

[1] Vgl. Art. 88 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] *Kühling/Buchner*, DS-GVO BDSG Kommentar, § 26 BDSG Rn. 3.

Mitarbeitern bis auf zwei Lageristen der Zutritt zum Lager und die eigenständige Entnahme von Ersatzteilen untersagt wurde. Mit den Lagermitarbeitern wurden auch Gespräche geführt. Eine Aufklärung der Fehlbestände war jedoch nicht möglich.

Aus diesem Grund ließ die Beklagte den Lagerraum mit Hilfe einer Videokamera überwachen. Kenntnis hiervon hatten nur die Lageristen und der Betriebsleiter. Der Betriebsrat wurde nicht beteiligt.

Auf den sodann erstellten Aufzeichnungen konnte beobachtet werden, wie ein Mitarbeiter (der spätere Kläger) Ersatzteile aus einem Regal entnimmt und mit diesen den Lagerraum verlässt. Aufgrund dieser Erkenntnisse wurden sodann eine außerordentliche sowie eine ordentliche Kündigung ausgesprochen. Hiergegen richtete sich die Kündigungsschutzklage des Klägers.

Die Vorinstanzen haben der Klage stattgegeben. Der Sachvortrag der Beklagten, der auf diesen Aufzeichnungen gestützt war, durfte nach Ansicht des LAG aufgrund eines Eingriffs in das Allgemeine Persönlichkeitsrecht des Klägers nicht verwertet werden.

## 2 Rechtsgrundlage eines Verwertungsverbotes

Zunächst eruiert das BAG die mögliche Rechtsgrundlage für ein Sachvortrags- oder Beweisverwertungsverbot. Ein solches Verbot ist nach BAG weder der ZPO noch dem Arbeitsgerichtsgesetz zu entnehmen. Denn in der Regel ist im Rahmen eines Gerichtsverfahrens der komplette Sachvortrag zu verwerten. Dies gebieten der Anspruch auf rechtliches Gehör gemäß Art. 103 Abs. 1 GG sowie § 286 ZPO, wonach das Gericht den gesamten Inhalt *„der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme“* bei seiner Entscheidung berücksichtigen muss (§ 286 ZPO).

Das BDSG wiederum enthält zwar Vorschriften über die Zulässigkeit der Verarbeitung von personenbezogenen Daten, jedoch keine dahingehende Sanktion, wonach Erkenntnisse, die unter Verstoß gegen BDSG gewonnen wurden, einem Sachvortrags- oder Beweisverwertungsverbot im Prozess unterliegen. Zu der alten Fassung des BDSG hatte das BAG entschieden, dass dessen Vorschriften zwar eine Konkretisierung des Schutzes *„des Rechts auf informationelle Selbstbestimmung und am eigenen Bild“,* jedoch keine Anordnung enthalten *„dass unter ihrer Missachtung gewonnene Erkenntnisse oder Beweismittel bei der Feststellung des Tatbestands im arbeitsgerichtlichen Verfahren vom Gericht nicht berücksichtigt werden dürften“*.[3]

[3] BAG, Urt. v. 29.6.2017 – 2 AZR 597/16, NJW 2017, 2853, Rn. 22.

Als Legitimation für die Annahme eines Beweis- oder Sachverwertungsverbotes bleibt nach BAG nur der zwingend gebotene Schutz des Allgemeinen Persönlichkeitsrechts mit seinen besonderen Ausprägungen (Art. 1 Abs. 3 und Art. 2 Abs. 1 GG). Denn bei der Urteilsfindung sind die Gerichte an die Grundrechte gebunden, so dass Erkenntnisse, die durch einen Eingriff in das allgemeine Persönlichkeitsrecht eines Betroffenen gewonnen worden sind, möglicherweise gegen diesen nicht verwendet werden dürfen. Hierbei kommt nach Auffassung des BAG nicht nur ein Beweis-, sondern sogar ein Sachvortragsverwertungsverbot (Nichtbeachtung unstreitigen Sachvortrags) in Betracht.[4]

Das Allgemeine Persönlichkeitsrecht umfasst nicht allein die Privat- und Intimsphäre, sondern auch das Recht am eigenen Bild und das Recht auf informationelle Selbstbestimmung.[5] Danach kann jeder Mensch selbst über die Preisgabe und Verwendung persönlicher Daten entscheiden. Ob ein Eingriff in das allgemeine Persönlichkeitsrecht stattgefunden hatte, prüft sodann das BAG anhand des Regelungswerks des § 32 BDSG a.F.

## 3 Zulässigkeit der Datenverarbeitung nach BDSG

Die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis setzte nach § 32 Abs. 1 S. 2 BDSG a.F. voraus, dass Anhaltspunkte für eine Straftat im Beschäftigungsverhältnis gegeben waren, die Maßnahme erforderlich war und das schutzwürdige Interesse des Arbeitnehmers an dem Ausschluss dieser Maßnahme nicht überwiegte, insbesondere die Maßnahme nicht unverhältnismäßig war.[6]

### 3.1 Verdacht einer Straftat

Nach dem Wortlaut des § 32 Abs. 1 S. 1 BDSG a.F. bedurfte es zunächst für die Datenverarbeitung des Verdachtes einer Straftat im Beschäftigungsverhältnis. BAG sieht einen Eingriff in das Recht am eigenen Bild aber auch dann als gerechtfertigt, wenn *„nur“* der konkrete Verdacht einer *„anderen schweren Verfehlung zulasten des Arbeitgebers“*[7] gegeben ist. Nach dem Urteil des BAG entfaltete § 32 Abs. 1 S. 2 BDSG a.F. keine *„Sperrwirkung“* gegenüber der Erlaubnisnorm des Satzes 1, mit der Folge, dass eine verdeckte Videoüberwachung auch beim Verdacht einer schweren Pflichtverletzung

[4] Vgl. LAG Hessen, Urt. v. 21.9.2018 – 10 Sa 601/18, K&R 2019, 213, wonach ein Verstoß gegen § 32 Abs. 1 S. 1 BDSG a.F. dazu führt, dass sogar der unbestrittene Inhalt einer E-Mail nicht verwertet werden kann, anhängig beim BAG unter dem Az. 2 AZR 564/18.

[5] Vgl. BVerfG, Urt. v. 11. 3. 2008 – 1 BvR 2074/05, 1 BvR 1254/07, NJW 2008, 1505, Rn. 61.

[6] Der Wortlaut des § 32 Abs. 1 S. 2 BDSG a.F. wurde größtenteils in § 26 BDSG n.F. übernommen.

[7] BAG, Urt. v. 20.10.2016 – 2 AZR 395/15, NJW 2017, 1193, Rn. 22.

eingesetzt werden kann, wenn die Verhältnismäßigkeit der Maßnahme gewährleistet ist.[8]

Der Wortlaut der Vorschrift – *„den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat"* – würde, für sich genommen, den Einsatz einer verdeckten Videoüberwachung erst dann erlauben, wenn sich der Verdacht auf den durch die Maßnahme Betroffenen beziehen würde. Das BAG entscheidet sich für eine großzügigere Auslegung. Der Verdacht müsse sich nicht *„gegen einen einzelnen, bestimmten Arbeitnehmer richten"*, sondern es reiche vielmehr aus, dass dieser *„einen zumindest räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern"* umfasst.[9] Das BAG sieht sich an diesem Auslegungsergebnis trotzt des Wortlautes der Vorschrift nicht gehindert. Dabei verweist es auf die Gesetzesbegründung, wonach das Regelwerk des § 32 BDSG a.F. die bisherigen Rechtsprechungsgrundsätze nicht ändern soll.[10] Es muss aus Sicht des BAG nur sichergestellt werden, dass der Kreis der Verdächtigen nicht durch weniger einschneidende Maßnahmen eingeschränkt werden kann.

Des Weiteren stellte sich die Frage, wie sicher es sein muss, dass eine Straftat begangen worden ist, bevor eine versteckte Videoüberwachung eingesetzt wird. Ein *„dringender Verdacht"* ist nach Auffassung des BAG nicht erforderlich. Ein *„einfacher Verdacht"* sei vielmehr ausreichend. Es müsse, mit anderen Worten, nicht mit großer Wahrscheinlichkeit feststehen, dass eine Straftat begangen worden ist. Es reiche vielmehr ein *„gewisses Maß an Konkretisierung und Verdichtung"*, so dass die Begehung einer Straftat *„nach der Lebenserfahrung"* möglich erscheint.[11]

Dieser Verdacht könnte vorliegend nach Auffassung des BAG gegeben sein, auch wenn andere Ursachen für die vorgetragenen Inventurdifferenzen nicht ausgeschlossen werden können. Nach dem BAG-Urteil hat das LAG den Vortrag der Beklagten – die Differenzen seien in kurzen zeitlichen Abständen aufgetreten, es seien leicht zu entfernende Teile betroffen, die anderen Maßnahmen hätten nicht geholfen – nicht ausreichend gewürdigt;

---

[8] BAG, Urt. v. 29.6.2017 – 2 AZR 597/16 NJW 2017, 2853, Rn. 28 ff.

[9] BAG, Urt. v. 20.10.2016 – 2 AZR 395/15, NJW 2017, 1193, Rn. 22.

[10] BT-Drs. 16/13657, S. 20 lautet auszugsweise: „§ 32 enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll". Eine abweichende Auffassung ist auch nicht der Gesetzesbegründung zu dem BDSG n.F. zu entnehmen, vgl. BT-Drs. 18/11325; In der Literatur ist diese Auffassung teilweise auf Kritik gestoßen, vgl. *Kühling/Buchner* (Fn. 2), § 26 BDSG, Rn. 59 mit Verweis auf *Brink*, in NK-ArbR § 32, Rn. 160.

[11] BGH, Beschl. v. 11.8.2016 – StB 12/16, StV 2017, 434 = BeckRS 2016, 15673, Rn. 9.

denn diese Angaben könnten einen hier ausreichenden *„Anfangsverdacht“* begründen.

### 3.2 Erforderlichkeit der Videoüberwachung

Nach Auffassung des BAG waren, unter Zugrundelegung des Vortrags der Beklagten, keine weniger einschneidenden, jedoch gleichermaßen erfolgversprechenden Maßnahmen ersichtlich. Der angestrebte Zweck der Aufklärung hätte man insbesondere nicht mit einer offenen Videoüberwachung erreichen können. In einem ähnlichen Fall hat das BAG ausgeführt: *„Derart auf Heimlichkeit angelegtes Verhalten kann seiner Natur nach nicht durch offen angekündigte Beobachtung entdeckt werden.“*[12]

### 3.3 Angemessenheit

Die Maßnahme ist nach Auffassung des BAG allgemein nicht unangemessen. Räumlich betreffe diese nur das Lager und somit genau den Ort, an welchem die vermissten Gegenstände aufbewahrt worden sind. Durch das Zutrittsverbot sei außerdem der Kreis der möglicherweise betroffenen Personen eingeschränkt worden. Wer trotzdem unbefugt diesen Bereich betrete, müsse den Eingriff hinnehmen.

### 3.4 Sonstige Gründe für ein Verwertungsverbot

Nach Ansicht des BAG kann sich der Kläger auch nicht darauf berufen, dass die Videoüberwachung möglicherweise das Allgemeine Persönlichkeitsrecht anderer Personen verletzt habe. Sinn und Zweck des § 32 BDSG a.F. bestehe nicht in einer Generalprävention.[13]

Auch ein Verstoß gegen die nach § 32 Abs. 1 S. 2 BDSG a.F. erforderliche Dokumentationspflicht[14] führt für BAG nicht zu einer Unverwertbarkeit des Sachvortrags. Sinn und Zweck dieser Dokumentationspflicht bestehe darin, die Rechtmäßigkeitskontrolle zu gewährleisten. Dieser Zweck könne aber auch dadurch erreicht werden, dass der Arbeitgeber in dem späteren Prozess die konkreten Anhaltspunkte für den Verdacht vorträgt.[15] Dies würde dann die bezweckte Rechtmäßigkeitskontrolle erlauben.

---

[12] BAG, Urt. v. 27.3.2003 – 2 AZR 51/02, NJW 2003, 3436.

[13] Vgl. zur Bestätigung dieses Grundsatzes auch LAG Baden-Württemberg Urt. v. 6.6.2018 – 21 Sa 48/17, BeckRS 2018, 30862, Rn 109: *„ist für die Zulässigkeit der Verwertung von Zufallsfunden eine datenschutzkonforme und daher rechtmäßige Erhebung von Daten auf Grund einer anderen Motivation heraus nicht notwendig“*.

[14] Dies gilt auch für § 26 Abs. 1 S. 2 BDSG. Nach der Rechtsprechung sind *„Schaden, Kreis der Verdächtigen und die Indizien“* zu dokumentieren, *Kühling/Buchner* (Fn. 2), § 26 BDSG, Rn. 60.

[15] So auch LAG Rheinland-Pfalz, Urt. v. 11.4.2019 – 5 Sa 371/18 (juris), und LAG Hamm Urt. v. 20.12.2017 – 2 Sa 192/17 (juris).

Ebenso wenig ergäbe sich ein Verwertungsverbot aus der fehlenden Zustimmung des Betriebsrates. Die Verletzung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG sei jedenfalls dann unbeachtlich, wenn die Datenverarbeitung nach *„allgemeinen Grundsätzen"* zulässig sei; denn in diesem Fall sei der auch mit dieser Vorschrift bezweckte Schutz des Allgemeinen Persönlichkeitsrechts erreicht, falls die Maßnahme etwa nach Maßnahme des BDSG zulässig sei.[16]

Die Entscheidung des Berufungsgerichtes wurde sodann aufgehoben. Nach Zurückverweisung der Sache an die Vorinstanz ist die Angelegenheit derzeit beim LAG Köln[17] anhängig.

## 4 Fazit

Mit dieser Entscheidung präzisiert das BAG die an einem Verdacht im Sinne des § 32 Abs. 1 S. 2 BDSG a.F. zu stellenden Anforderungen. Nach BAG ist der Einsatz einer heimlichen Videoüberwachung nicht nur beim Verdacht einer *„Straftat"*, sondern auch beim Verdacht einer *„schweren Verfehlung"* im Arbeitsverhältnis zulässig. Dies erlaube der Grunderlaubnistatbestand des § 32 Abs. 1 S. 1 BDSG a.F., denn § 32 Abs. 1 S. 2 BDSG a.F. entfalte insoweit keine Sperrwirkung. Dies erscheint konsequent. Eine schwere Pflichtverletzung kann für die Entscheidung bezüglich der Beendigung des Arbeitsverhältnisses von gleicher Bedeutung sein wie eine Straftat.

Die Grundsätze bezüglich des erforderlichen Verdachtsgrades stellen einerseits sicher, dass kein uferloser Einsatz von heimlichen Überwachungsmethoden zulässig ist. Andererseits eröffnen diese dem Arbeitgeber einen gewissen Beurteilungsspielraum, da dieser mit solchen Maßnahmen nicht so lange warten muss, bis eine an Sicherheit grenzende Wahrscheinlichkeit gegeben ist.

Hilfreich sind auch die Ausführungen bezüglich der Substantiierbarkeit des Sachvortrags des der Überwachungsmaßnahme einsetzenden Arbeitgebers. Dieser muss insbesondere das Gericht überzeugen, dass mildere und vergleichbar geeignete Mittel ausgeschöpft worden sind. Wenn eine weitere Einschränkung der Betroffenen durch mildere Mittel nicht möglich ist, darf die verdeckte Überwachungsmaßnahme eingesetzt werden.

Des Weiteren wird klargestellt, dass nicht jeglicher Verstoß gegen die Vorschriften des BDSG a.F. eine Unverwertbarkeit der sich aus der Über-

[16] So auch BAG, Urt. v. 31.1.2019 – 2 AZR 426/18, NJW 2019, 2883.

[17] LAG Köln, – 4 Sa 1198/14.

wachungsmaßnahme ergebenden Erkenntnisse nach sich zieht. Eine Unverwertbarkeit kommt erst dann in Betracht, wenn damit eine Perpetuierung eines Eingriffs in grundrechtlich geschützte Positionen stattfinden würde.

Man darf letztendlich mit Spannung abwarten, ob die Rechtsprechung diese Grundsätze auch nach Inkrafttreten der DS-GVO anwenden wird. In der Literatur wird die Auffassung vertreten, dass § 26 BDSG eine verdeckte Videoüberwachung nicht mehr erlauben würde.[18] Denn das in Art. 88 Abs. 2 DS-GVO verankerte Transparenzgebot könne nach Maßgabe des Art. 23 Abs. 1 DS-GVO nur durch eine gesetzliche Regelung eingeschränkt und eine solche könne nicht in Art. 26 BDSG hineingelesen werden.

[18] So *Kühling/Buchner* (Fn. 2), § 26 BDSG Rn. 22.

# THE NEW EUROPEAN ELECTRONIC COMMUNICATION CODE

Dr. Gerd Kiparski, MBA

1&1 Drillisch AG
Gerd.Kiparski@1und1.de

## Zusammenfassung

Telecommunication services form part of everyday life. The dependency on these kinds of services is continuously increasing and their complexity is increasing. New services like *WhatsApp* and *Skype* emerged and telecommunication operators today bundle a wide range of services and hardware into end user contracts. Therefore, the former legal telecommunication framework needed a refit to cope with new challenges, especially in the end user protection field. The new European Electronic Communication Code fully harmonizes the end user protection rules across Europe, covers for the first time new OTT-services and tries to make the end user protection rule futureproof.

## 1 A Long way to the new telecommunication code

The former European telecommunication framework consisted of four directives, the Access Directive,[1] the Authorisation Directive,[2] the Framework Directive,[3] and the Universal Service Directive.[4] These four directives date back to the year 2002. They have been amended in the year 2009 by the Better Regulation Directive[5] and the Citizens` Rights Directive[6] and were adjusted to new market trends. However, significant market trends, like the rise of Over-the-Top (OTT) services were in their infancy and therefore not covered by the amended directives.

The European law maker made its first steps towards modernizing the European telecommunication framework in the year 2013. Then, the European Commission published the telecom single market regulation (TSM), which had the approach to refit the framework and amend it in order to be fit for actual challenges.[7] The law making process took over two years and the Commission`s proposal was watered down to only two aspects, the net

---

1 Directive 2002/19/EC of 7.3.2002.

2 Directive 2002/20/EC of 7.3.2002.

3 Directive 2002/21/EC of 7.3.2002.

4 Directive 2002/22/EC of 7.3.2002.

5 Directive 2009/140/EC of 25.11.2009.

6 Directive 2009/136/EC of 25.11.2009.

7 COM(2013) 627 final. A detailed analysis provided by *Gerpott*, K&R 2013, p. 781 (781 ff.).

neutrality and the Roam-like-at-home regulations.[8] Therefore, the need to adapt the current framework to new market conditions remained even after the TSM regulation entered into force.

The European Commission started a new approach in 2016 and published the draft European Electronic Communication Code directive.[9] The aim of this directive is inter alia to cover OTT-services as well and to harmonize to consumer protection level across the EU.[10] After two years of law making process the final Codex was published in the official journal of the EU on December, 17th, 2018.[11] The new codex replaces the current four directives and provides new rules for investments and rollout of very high speed networks, competences of the *Body of European Regulators of electronic Communication* (BEREC) and frequency allocation. However, this article will focus on the harmonized consumer protection regime in the new Code.

## 2 OTTs are now in Scope

Electronic communication services were previously defined in Art. 2 lit. c Framework directive as services consisting wholly or manly in the conveyance of signals via electronic communication networks. This definition did not cover OTT services as the ECJ recently decided, since OTT-operators only use signal transmission of internet access providers. They provide their services via the open internet, but they don`t have any control of the underlying signal transmission.[12] Furthermore, the signal transmission cannot be attributed to the OTT operator since OTT operators usually don`t have a contractual relationship to network operators.[13] Therefore, services like *WhatsApp*, *Facebook Messenger* and *Skype* do not qualify as electronic communication services according to Art. 2 lit c Framework directive with the legal telecommunication framework not applying to them.[14]

According to the aim of the new Code to create a level playing field between OTTs and classic telecommunication services the definition of electronic communication services in Art. 2 para 4 of the Codex was extended

---

8 See the Telecom Sigle Market Regulation (EU) 2015/2120 of 25.11.2015.

9 COM(2016) 590 final. Indepth comments on the draft: *Gerpott*, K&R 2016, p. 801 (801 ff.); *Scherer/Heckmann/Heinickel/Kiparski/Ufer*, CR 2017, p. 197 (197 ff.); *Neumann*, N&R 2016, p. 262 (262 ff.); *Scherer/Heinickel*, MMR 2017, p. 71 (71 ff.).

10 Recital 5 of the Codex.

11 OJ No. L 321 of 17.12.2018, p. 36-214.

12 ECJ, 13.6.2019 – C-193/18 (Gmail), CR 2019, 464; See as well for SkypeOut: ECJ 5.6.2019 – C-142/18, CR 2019, 466.

13 ECJ 5.6.2019 – C-142/18, CR 2019, 466 (468).

14 See *Kiparski*, CR 2019, p. 460 (464).

and encompasses now internet access services, interpersonal communication services and services consisting wholly or mainly in the conveyance of signals.[15]

Interpersonal communication services are defined in Art. 2 para. 5 of the Code as services normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communication networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipients.

Interpersonal communication services are split into number-based (Art. 2 para. 6) and number-independent (Art. 2 para. 7) services, whereby OTT-services form part of the number-independent interpersonal communication services.[16]

## 3 End User Rights

End user rights have been part of the legal framework since 2002. However, since the framework was a directive, the end user rights established a bottom line. Member States could deviate to the benefit of consumers. This led to different end user protection rules across all Member States and became an obstacle for pan-European-services.[17] Therefore, the Code foresees now in Art. 101 para. 1 a full harmonization of the end user protection rules without allowing more or less stringent rules in the member States. Importantly, this full harmonization applies only to those aspects covered by the Code and not to national rules which deal with aspects the Code doesn`t cover.[18] Therefore, when implementing the Code, Member States have to carefully evaluate, whether a national regulation has the same scope as a regulation in the Code or whether it deals with different aspects.

The Code has to be implemented into national law according to Art. 124 No. 1 until December 21st, 2020. Regarding end user rights the Code provides in Art. 101 para. 2 the ability for Member States to keep more stringent end user protection rules until December 21st, 2021 providing one additional year grace period.

The aim of harmonizing end user rights across Europe is to increase legal certainty for both end users and providers of electronic communication and

[15] *Kiparski*, CR 2019, p. 179 (180); *Neumann*, N&R 2019, p. 152 (153).

[16] *Neumann*, N&R 2019, p. 152 (153).

[17] Recital 257 of the Code. See as well *Kiparski*, CR 2019, p. 179 (184).

[18] Recital 257 of the Code. See as well *Neumann*, N&R 2019, p. 152 (158).

thereby to lower entry barriers and unnecessary compliance burdens stemming from fragmentation of the national rules.[19]

### 3.1 Information Obligations

The new Code provides in Art. 102 a wide variety of information that operators have to provide. This obligation applies to all providers of electronic communication services and therefore to OTT operators as well. Already the former framework provided a broad information obligation for operators. However, the new Code extends the level of information with certain quality of service information and sets the first milestone of information provisioning quite early in the contract conclusion process.

There is a set of information that has to be provided even before a consumer is bound by a contract or any corresponding offer. This information is outlined in Annex VIII of the Code and contains e.g. the minimum level of quality of the service, latency, jitter and packet loss the price, the contract duration and the information set out in Art. 4 para 1 of the TSM directive.[20]

Prior to the conclusion of a contract operators have to provide consumers according to Art. 102 No. 3 with a contract summary. The contract summary has to include the operator`s name and address, the characteristics of each service provided, the respective price, the duration of the contract and conditions for termination and information about the service quality according to Art. 4 para. 1 lit. d and e of the TSM directive. The information provided becomes according to Art. 102 No. 4 an integral part of the contract. BEREC will provide a template of a contract summary which operators may us to fulfil their obligation.

### 3.2 Comparison Tool

New in the Code is the obligation for Member States to have at least one independent and free of charge comparison tool, which according to Art. 103 para 2 enables end users to compare and to evaluate different internet access services and number-based interpersonal communication services. The comparison toll shall be open to any provider and have clear and objective criteria on which the comparison is based. End users shall have the ability to compare prices, tariffs and quality of service performance. Operators of comparison tool on the other hand have the right to use, free of charge the information published by providers of internet access services and publicly available interpersonal communication services for the purpose of making available such independent comparison tool.

[19] Recital 257 of the Code.

[20] See for details: *Kiparski*, CR 2019, p. 179 (184).

The aim of introducing comparison tools together with detailed rules about operator switching and the reduction of notice periods in case of termination is to foster competition amongst operators and to make it more easy and convenient for customers to switch operators.

### 3.3 Contract Duration and Termination

The new Code sets a new standard for contract duration and termination of electronic communication contracts. So far, the legal framework limited in Art. 30 para. 5 of the Framework directive the initial maximum loyalty period to 24 months. The Code provides as well in Art. 105 para 1 an initial maximum loyalty period of 24 months. However, in para. 3 of Art. 105 the Code provides as well a regulation for automatic prolongation. Automatic prolongations remain possible, but end users have a termination right during that automatic prolongation period of maximum one month notice period. The Code speaks misleadingly in Art. 105 para. 3 of an automatic prolongation of a fixed duration contract. In practice, there are no fixed duration contracts that get prolonged. Operators use contracts of undefined terms and exclude the right to terminate for a certain period of time. Therefore, Art. 105 para. 3 of the Code has to read in a manner that it applies as well to contracts of indefinite terms with a 24 month exclusion of the right to terminate.[21]

Furthermore, operators have to inform end users in a prominent manner accordingly before the contract is automatically prolonged, according to Art. 105 para. 3 of the Code.[22] The regulations of the contract duration do not apply to OTT services since the scope of Art. 105 is limited to publicly available electronic communication services other than number-independent interpersonal communication services.[23]

### 3.4 Amendments of Terms & Conditions

According to Art. 105 para. 4 operators may change the conditions of the contract with an end user.[24] The right to amend the contractual conditions is not limited to certain conditions. Therefore, operators may at any time proceed with contract amendments following the process outlined in Art. 105 para. 4. In case of a contract change, the provider has to notify the end user at least one month in advance and inform the end user accordingly of his right to terminate the contract without any incurring or further costs. The right to terminate the contract may be exercised by the respective end

[21] *Kiparski*, CR 2019, p. 179 (185).

[22] See *Kiparski*, CR 2019, p. 179 (186).

[23] See *Kiparski*, CR 2019, p. 179 (185).

[24] *Kiparski*, CR 2019, p. 179 (186).

user within one month after notification of such change. The end user has no right to terminate the contract, if the changes are exclusively to his benefit, if they are purely administrative nature and have no negative effect on the end user or if they are directly imposed by law.

### 3.5 Provider Switching and Number Portability

The provider switching process is regulated quite detailed in Art. 106 of the Code. Previously, Art. 30 of the Universal Service directive provided the right for end users to switch operators and to port their number from one operator to another. Already the former switching process allowed a down time for the end user of maximum one day. The new Code keeps the end user right to switch and port his number, however extends the downtime to one working day. Now downtimes during weekends and national holiday do not count and operators can initiate a switching process even before weekends and national holidays without having an emergency team ready during that time. On the other hand, the new Art. 106 para. 6 determines that the new operator leads the switching process in order to make it more easy and smooth for the end user. Single point of contact for the end user will be the new operator who has to deal with the end user`s former operator. If the operator switching process fails, according to Art. 106 para. 5 the previous operator has to take the customer back and activate his number and the services again and keep them going until the switching to the new operator is successful.

End users already have the right to port their number to their new operator during the switching process. According to Art. 106 para. 3 end users may as well decide to port their number after the switching occurred. Within a period of one month after termination of the previous contract an end user can still request the porting of his number to his new operator. The number porting will be free of charge for end users, Art. 106 para. 4. Today, many European operators charge for number porting.[25]

For the first time, the Codex allows in Art. 106 para. 6 end users of prepaid services to reclaim any credit after the laps of the contract. Operators have to refund any credit, but may charge for the refund a fee which is proportionate to the incurred costs.[26]

[25] In Germany operators charge for the porting of a mobile number on average between 29 and 30 Euro, for a fixed number the NRA set the price on 11,44 Euro.

[26] See *Kiparski*, CR 2019, p. 179 (186).

### 3.6 Bundled Offers

Telecommunication providers bundle their telecommunication services with a variety of other services. Nowadays, triple-play offers gain customers` attraction, for which operators bundle fixed and mobile with TV services. On top, these services get bundles with hardware like smartphones, set-top-boxes and routers. Furthermore, providers offer top-up services like special roaming packages or zero-rating services.

Since these offers are popular amongst end users but they provide some down-sides, like contractual lock-in,[27] the new Code regulates bundled offers for the first time in Art. 107. A bundled service is defined in Art. 107 para. 1 as a bundle of services or a bundle of services and terminal equipment offered to a consumer which comprises of at least an internet access service or a publicly available number-based interpersonal communication service. First of all, OTT services are not in scope of this regulation. Secondly, to qualify as a bundle according to Art. 107 para. 1 the bundle must be offered to a consumer, meaning the offer should be in one contract or at least in several contracts concluded at the same time.[28] If the customer adds later different services to his internet access service, these do not qualify as a bundle.

The legal consequence of a bundle according to Art. 107 para. 1 is that Art. 102 para. 3, Art. 103 para. 1 and Art. 105 and Art. 106 para. 1 apply mutatis mutandis to all elements of the bundle. Hence, the operator has to include the bundled elements into his contract summary according to Art. 102 para. 3, the bundle forms part of the maximum contractual period of 24 months according to Art. 105 and the termination regime during contractual prolongation and furthermore, the bundle forms part of the operator switching process according to Art. 106 para. 1 meaning that the entire bundle can`t be switched off, if the switching process was not successful.

The initial loyalty period of a running contract shall not be extended or re-started, if the customer decides later to subscribe to additional services or equipment.[29] Art. 107 para. 3 provides that the original duration of the contract shall remain as is, even if the customer adds additional services or hardware. Of course, Art. 107 para. 3 provides as well, that if a customer deliberately decides to prolong his or her contract in order to e.g. receive a new smartphone, the loyalty period contract may be prolonged. However, this is possible only by an expressly agreement with the customer.

---

[27] Recital 283 of the Code.

[28] See *Kiparski*, CR 2019, p. 179 (187).

[29] *Kiparski*, CR 2019, p. 179 (187).

### 3.7 Intra-EU Communication

BEREC performed two studies with the outcome that there are significant discrepancies in the price customers pay for national calls and SMS and the costs for international calls and SMS to other Member States of the EU.[30] The European Commission concluded that these price discrepancies are to the detriment of the Single Market.[31] Therefore, the European Commission decided to amend the TSM directive and introduce price caps for intra-EU communication. Regulated Intra-EU communication is defined in the amended Art. 2 para. 3 of the TSM directive as a number based communication service originating in one Member State of the customer`s domestic provider and terminating at any fixed or mobile number of another Member State. The Commission used the new BEREC directive[32] to amend the TSM directive. In Art. 50 of the BEREC directive a new Art. 5a is introduced to the TSM directive. According to Art. 5a the retail price for consumers for communication to another Member State of the European Union shall not exceed 19 Cent per Minute for voice calls and 6 Cent per SMS, each excluding VAT. MMS services are not regulated and therefore not price caped.

Operators are still free to offer other tariffs for international calls, as long as they ensure that the default price plan are the regulated intra-EU communication prices. Customers may deliberately and expressly opt for a different price plan than the regulated intra-EU prices according to Art. 5a para. 2. However, according to Art. 105 para. 4 consumers may switch back to the regulated tariff within one working day free of charge.

The price cap for Intra-EU communication applies according to Art. 5a form May, 15th 2019 onwards.

[30] BEREC BoR (18) 41 and BoR (18) 75.

[31] Recital 43 of directive (EU) 2018/1971 of 11.12.2018 (BEREC directive).

[32] Directive (EU) 2018/1971 of 11.12.2018.

## Literatur

*Gerpott, Torsten:* Regulierungsvorschlag der Kommission zur Verwirklichung eines integrierten europäischen Telekommunikationsmarktes, K&R 2013, p. 781-787.

*Gerpott, Torsten:* Vorschlag der Kommission zur Weiterentwicklung des europäischen Rechtsrahmens für den Telekommunikationssektor, K&R 2016, p. 801-808.

*Kiparski, Gerd:* Der europäische Telekommunikations-Kodex – Ein neuer Rechtsrahmen für die elektronische Kommunikation, CR 2019, p. 179-188.

*Kiparski, Gerd:* Der EuGH schafft Klarheit: OTT-Dienste sind in der Regel keine Telekommunikationsdienste, CR 2019, p. 460-464.

*Neumann, Andreas:* Der Kommissionsvorschlag für einen europäischen Kodex für die elektronische Kommunikation, N&R 2016, p. 262-272.

*Neumann, Andreas:* Erste Schritte auf dem Weg zur Umsetzung des europäischen Kodex für die elektronische Kommunikation – Die Eckpunkte zur TKG-Novelle 2019, N&R 2019, p. 152-162.

*Scherer, Joachim/Heinickel, Caroline:* Ein Kodex für den digitalen Binnenmarkt, MMR 2017, p. 71-77.

*Scherer, Joachim/*Heckmann, *Dirk/Heinickel, Caroline/Kiparski, Gerd/Ufer, Frederic:* Stellungnahme der DGRI zum Vorschlag der Europäischen Kommission für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation (COM[2016]590 final), CR 2017, p. 197-202.

# 5G NETWORK ECONOMICS: FROM MARKETING STRATEGY TO IOT AND BLOCKCHAIN NETWORK SLICING REGULATIONS

Alexis Daj

Transilvania University of Brasov - Faculty of Economic Sciences and Business Administration
alexis.daj@unitbv.ro

## Summary

The 5G ecosystem (as a network of networks) is just the inception of a new paradigm after the historically successful expansion of mobile communication systems in the last 25 years. The 5G powered future promises to provide a superior end-user experience by delivering new applications and services through gigabit speeds, and notably superior network performance and reliability. Consolidating the successes of 2G (GSM), 3G (UMTS) and 4G (LTE) mobile networks, 5G Smart Networks are of strategic importance as the enabler for fundamentally all sectors in society and economy for jobs and economic growth, through supporting novel services and innovative business models, being even capable of changing whole societies. Spectrum is an essential element of wireless networks that support the communication services people and companies use every day. The myriad of novel 5G services and applications, will necessitate in the near future a diverse set of spectrum bands, with distinctive features, addressing different requirements, and mixing both low and high frequencies. Therefore, there is a vigorous preoccupation of governments and regulators for efficient allocation and use of 5G spectrum. Moreover, given also the advance of groundbreaking network management technologies (such as Cognitive Radio, Blockchain and Network Slicing), we can anticipate that spectrum sharing will be a leading area for innovation, standardization and spectrum regulation in the next few years and beyond, especially as network slicing guarantees a virtually endless adaptation of network-spread functionality, while the decoupling of the platform supplying the service and the service elements reaches a new level.

## 1 Introduction

As the Digital Revolution is well under its way, some essential questions arise regarding the interactions behind technological, legal and economic forces that drive these complex processes and the evolution of the theoretical background.

The novel technologies developed around the 5G network standard have a tremendous potential to offer very powerful instruments for both businesses and regulatory authorities which will profoundly impact business models and will allow a more efficient and dynamic use of scarce resources like radio frequency spectrum.

One of the major outcomes of the 5G network implementation (centred on the Internet of Things - IoT) is the development of the fourth industrial revolution, also referred to as Industry 4.0, that - according to the Boston Consulting Group (2019) and industrial systems thinker Olivier Scalabre - "will produce a macroeconomic shift and boost employment, productivity, and growth" through making "production systems up to 30 % faster and 25 % more efficient", while bringing mass customization to unprecedented levels.[1]

The following sections will cover the theoretical background of network economics - highlighting the specific features of network industries and platform markets, and will give an overview of digital transformation and 5G requirements - also identifying 5G regulatory challenges and the role for antitrust.

## 2 Theoretical Background - Network Economics

### 2.1 Network Industries and Platform Markets

When regulation authorities and business strategists develop policies and marketing strategies in connection with IoT and next generation 5G networks, they have to take into account the economic specificities of this intricately connected environment - namely, network effects generated by network industries and platform markets.

According to Phil Weiser,[2] there are two main definitions of the concept of **network industry:**

a) A general, *broad definition* which considers a network industry to be "an industry that connects users to each other or to producers through a connected system (or systems) of physical infrastructure" having as main examples "communications networks, power grids, transportation systems, and software platforms".
b) A *narrow definition* (or an economic definition) that describes a network industry as "an industry whose good or service increases in value to each individual user as the number of other users of the same good or service increases" with a reduced set of cases like "communications networks, software platforms, and transportation systems".

[1] Boston Consulting Group (BCG), Embracing Industry 4.0 and Rediscovering Growth, 2019. Available at: https://www.bcg.com/en-ao/capabilities/operations/embracing-industry-4.0-rediscovering-growth.aspx (last access: 20.7.2019).

[2] *Weiser*, Network Economics 101, Aspen, Colorado, April 29, 2007. Available at: http://www.pff.org/issues-pubs/testimony/2007/070430IRLE2007networkeconomics101.ppt. (last access: 20.7.2019).

Other researchers like Nicholas Economides stress that there are market settings in which - even without the reliance on a physical network - we can identify so called **virtual networks** that consist of a "collection of compatible goods that share a common technical platform" (e.g. the ensemble of all VHS video players or of all computers running the Windows operating system). Therefore, the "crucial defining feature of networks is the complementarity between the various nodes and links" they are made of.[3]

Furthermore, we can consider the basic economic definition proposed by Claude Crampes for a network:

*"A network is a set of points (or nodes) and interconnecting lines (or edges) organised with the object of transmitting flows of energy (electricity, heat), information (sound, data, pictures) or material (water, freight, passengers, etc.). Each point can be an initial node from which the flow is emitted, a terminal node, receiving the flow, or a node that plays an intermediary role of transmission, storage, amplification, co-ordination, dispatching and so on. Some networks are one-way, like gas, cable TV and water delivery while others are two-way, like passenger transportation or telephone."*[4]

Claude Crampes concludes that the quintessence of a network structure is reflected by the "multiple potential links" which allow "that (almost) every pair of nodes can be linked by more than one line" with the consequence that "the best network is the one that minimises total costs". Thus, "the design of a network results from a trade-off between building costs and operating costs".

In this context, we have to highlight the role of platform markets - another important concept related to 5G technologies, which will represent one of the underpinnings of platform-oriented business models. According to Weiller and Pollitt, a "**platform market** is a market where user interactions are mediated by an intermediary, the platform provider, and are subject to network effects". Moreover, they accentuate that, differently from a classic marketplace or simple trading exchange, "a platform intermediary must offer inherent value beyond the simple mediation process for the two sides of the market" with the added-value generally created by "ICT and

[3] *Economides*, Notes on Network Economics for the MBA class "Networks, Telecommunications Economics, and Digital Convergence", September 2003, p. 4. Available at: http://neconomides.stern.nyu.edu/networks/Netnotes_2003.pdf (last access: 20.7.2019).

[4] *Crampes*, Network Industries and Network Goods (Introductory chapter to a study for the European Commission), IDEI, September 1997, p. 3. Available at: http://idei.fr/sites/default/files/medias/doc/by/crampes/network.pdf (last access: 20.7.2019).

the associated complementary innovation that increases utility and attractiveness of the platform to all user groups".[5]

Bertin points out that the traditional economic term used to describe platform markets is that of "**two-sided"** or "**multi-sided" markets (MSM)** where two or more categories of users (e.g. buyers and sellers, advertisers, software developers, social media users, etc.) are linked by a platform to enable an exchange or a transaction. Bertin stresses that network effects are not the most significant feature of platforms. Therefore, "platforms can be more narrowly defined as a place where two or more types of users can directly interact with each other, facilitated and observed by the platform operator", in order to differentiate them from *retailers* ("where no direct interaction is possible"), or from *vertically integrated firms* ("that integrate one side of the market under a single ownership structure"). Consequently, Bertin discusses several examples of platform mechanisms: "For instance on AirBnB real estate owners and clients can interact directly to conclude a deal. [...] Some platforms operate hybrid business models that combine these characteristics. Amazon is both a retailer and a platform; it is also a vertically integrated firm that operates warehouses and logistics services. Apple produces hardware and software. Netflix produces and distributes films. These platforms are vertically integrated production chains on one side of the market. They may operate as a retailer for another part of the market and have a true platform market place for still other parts of the market."[6] Further examples of platform markets can be seen in Fig. 1.

[5] *Weiller/Pollitt*, 2013. "Platform Markets and Energy Services", Cambridge Working Papers in Economics 1361, Faculty of Econom-ics, University of Cambridge, p. 7. Available at: https://www.eprg.group.cam.ac.uk/wp-content/uploads/2013/12/1334-PDF.pdf (last access: 20.7.2019).

[6] *Martens*, An Economic Policy Perspective on Online Platforms, Institute for Prospective Technological Studies Digital Economy Work-ing Paper 2016/05. JRC101501, p. 3. Available at: https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf (last access: 20.7. 2019).

*Fig. 1: Examples of platform markets (Energy Policy Research Group)*[7]

Other researchers like Hagiu and Wright advocate an additional narrowing of the MSM demarcation to a **market place** where users participate with a *sunk cost* in their membership process to the platform while users on opposite sides of the market are able to directly interact with each other. Moreover, Hagiu and Wright add a *vertical integration aspect* and differentiate between *market places* (which allow buyers and sellers to communicate more freely) and *retailers* or *re-sellers* (which take control of the transaction). Furthermore, the vertically integrated firm establishes a distinct group in the Hagiu-Wright classification because the platform operator "owns" the supplier. In this line of thought, retailers and vertically integrated firms are not included in the in their definition of an MSM (see Fig. 2).[8]

[7] Energy Policy Research Group, Electricity markets as platform markets, 2014. Available at: http://www.eprg.group.cam.ac.uk/wp-content/uploads/2013/10/Slides-for-EPRG-meeting.pptx (last access: 20.7.2019).

[8] *Hagiu/Wright*, "Multi-Sided Platforms." International Journal of Industrial Organization 43 (November 2015): 162–174, p. 6. Available at: https://www.hbs.edu/faculty/Publication%20Files/15-037_cb5afe51-6150-4be9-ace2-39c6a8ace6d4.pdf. (last access: 20.7.2019).

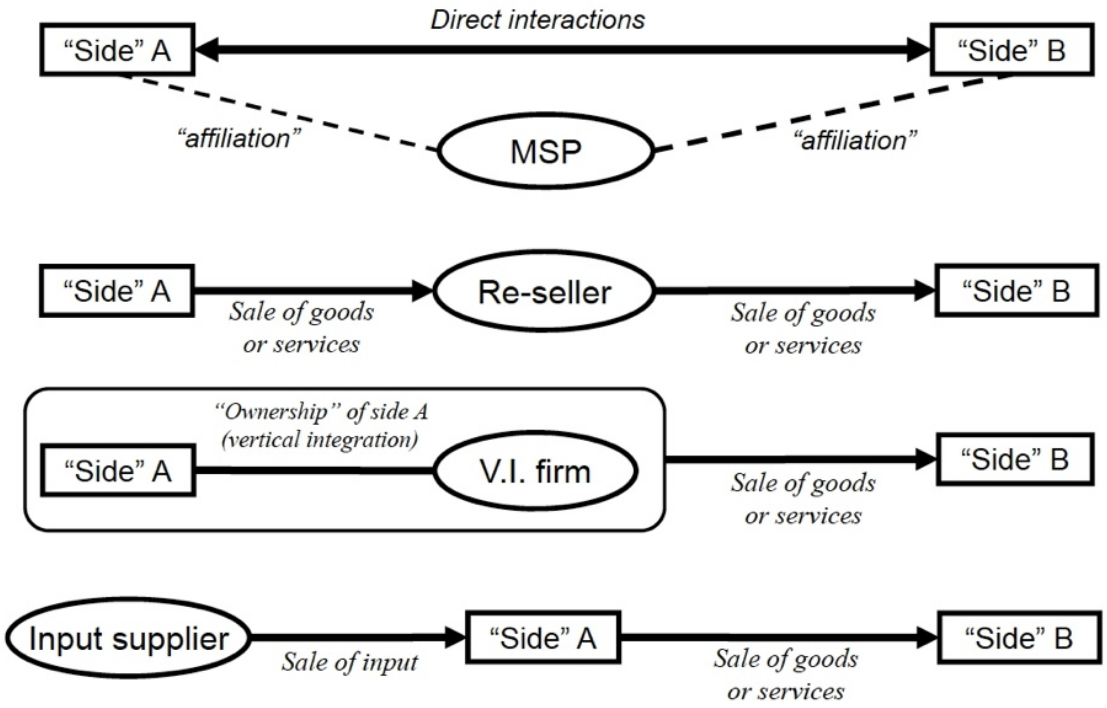


*Fig. 2: MSMs vs. alternative business models (Hagiu/Wright, 2015)*

Eisenmann, Parker, and Van Alstyne – while underlining that there isn't always a sole company which establishes and manages a platform – identify three "*supply roles*":[9]

a) **Platform providers** – acting as first "point of contact", they intermediate network users' interactions;
b) **Component suppliers** (co-developers) – that provide essential goods and services that are not supplied directly by platform providers; and
c) **Platform sponsors** – which are endowed with control rights and, thus, able to alter platform technology and regulate who may partake in the network.

[9] *Eisenmann et al*, Platform Networks – Core Concepts: Executive Summary, MIT Center for Digital Business, Paper 232 (June 2007), p. 3. Available at: http://ebusiness.mit.edu/research/papers/232_VanAlstyne_NW_as_Platform.pdf. (last access: 20.7.2019).

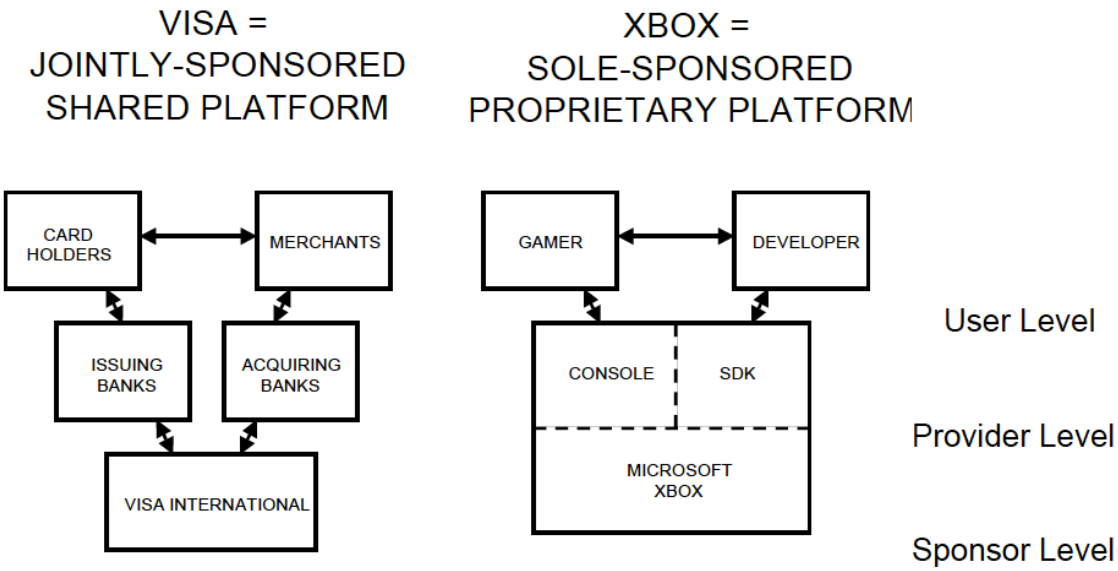


*Fig. 3: Comparison of VISA and Xbox Platforms (Eisenmann et al., 2007)*

Platform sponsors can license several platform providers to encourage innovation (usually under the patronage of an association - e.g., VISA, which is operated by 21,000 affiliate banks) or retain this role for themselves (instances of platforms with a single sponsor comprise Apple's Macintosh and the American Express credit card or Xbox). (See Fig. 3.)

## 2.2 Network Effects and Competitive Behaviour

While in classic non-network industries the law of demand implies that a consumer is willing to pay less for the last unit of a good as the number of units sold increases, in markets that generate network effects the inclination to pay for the last unit may be higher as more units are sold (i.e. for some sectors the demand curve has a positive slope, showing that, as sales increase, people are prepared to pay more for the last unit). Economides considers that "the key reason for the appearance of network externalities is the complementarity between network components" and that, "depending on the network, the network effect may be *direct* or *indirect*".[10]

In other words, the existence of a **network effect** implies that the value of a service or product increases when the number of people who use it rises, thereby boosting the numbers of consumers. A well-known illustration of this phenomenon - when the value of a product or service is related to the number of others using it - is the telephone network: the more people own telephones, the more valuable is the telephone to each owner.

Network effects represent **demand-side scale economies** as they impact existing and prospective users' susceptibility and willingness-to-pay for

[10] *Economides*, Notes on Network Economics for the MBA class "Networks, Telecommunications Economics, and Digital Convergence", September 2003, p. 9.

platform membership.[11] Nevertheless, **demand-** and **supply-side economies** are conceptually distinct: unit cost reductions that result from network growth should not be labelled "network effects".

A mathematic correlation between the number of users and the value of the products or services associated with the network was developed by Robert Metcalfe during the 1970's when network effects were first studied in the context of long-distance telephony. **Metcalfe's Law** says that the *systemic value of a network* is proportional to the square of the number of devices connected to the network. (See Fig. 4.)

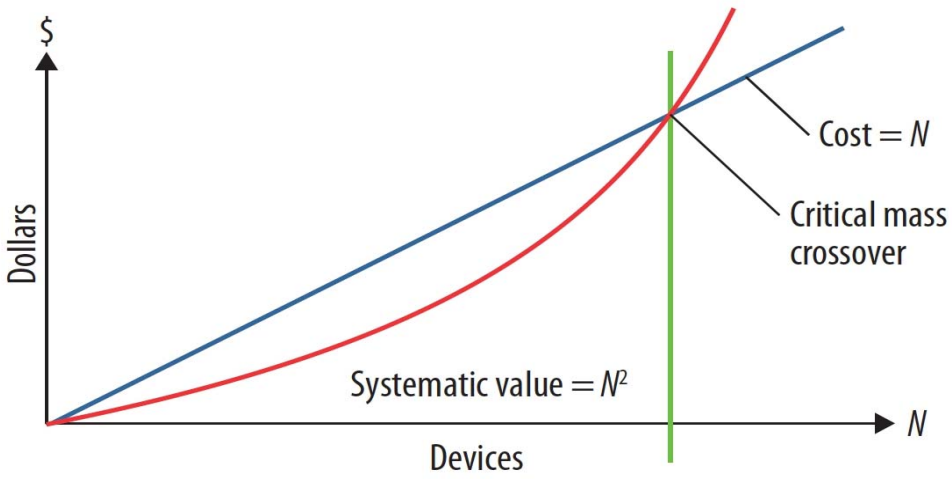


*Fig. 4: Graph showing that the systemic value of a network is proportional to the square of the number of devices connected to the network. (SOURCE: Metcalfe, 2013)*[12]

As mentioned earlier, there are two main types of network effects:

a) **Direct network effects** - are the simplest form of network effects where the growth in the usage generates the direct rise in the value (as in the case of the telephone service); and
b) **Indirect network effects (or two-sided effects)** - these imply that´increases in usage by one set of users augments the value of a complementary product to another different set of users, and vice versa (as in the case of hardware/software platforms, or reader/writer software pairs).

From a **competitive behaviour** perspective, the capacity to determine prices on both sides of a network makes complex pricing strategies possible and, therefore, generates a topic that has been in the focus of formal economic research. Regarding pricing in two-sided markets, Rysman summarises the difference between two-sided markets and one-sided markets as follows:

[11] *Eisenmann et al*, Platform Networks – Core Concepts: Executive Summary, MIT Center for Digital Business, Paper 232 (June 2007), p. 2.

[12] *Metcalfe*, Metcalfe's law after 40 years of Ethernet, IEEE Computer 2013, p. 26 (28).

*"The main result is that pricing to one side of the market depends not only on the demand and costs that those consumers bring but also on how their participation affects participation on the other side and the profit that is extracted from that participation. In a one-sided market, we can characterize the price– cost mark-up in terms of elasticity of demand and the marginal cost. But in a two-sided market, pricing decisions will also include the elasticity of the response on the other side and the mark-up charged to the other side."*[13]

As a business is able to earn money from either side of the network, adapting profits in two markets becomes possible: subsidizing market one can increase demand and profits in market two more than the loss in market one. (See Fig. 5.)

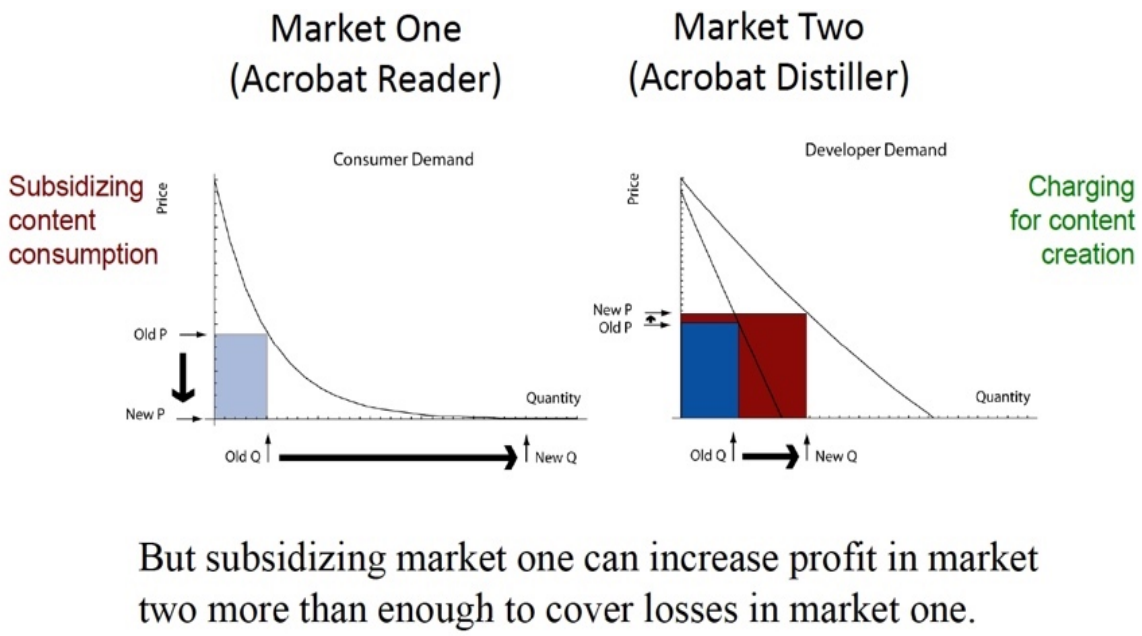


*Fig. 5: Adapting profits in two markets. (SOURCE: Eisenmann, Parker and Van Alstyne)*

An eloquent example would be the case of Adobe, which distributes its two software products according to the different market sides: the *Acrobat Reader* as freeware, while it makes its profits from the *Acrobat Distiller* product that allows the generation of files that can be read by the Acrobat Reader.[14]

From a **regulatory point of view**, regulation authorities can force firms to share their network externality (e.g. through an interconnection or interoperability order), because network externalities can generate lock-in by making the alternative provider less appealing in terms of the benefit it will

[13] *Rysman*, The Economics of Two-Sided Markets, Journal of Economic Perspectives 2009 p. 125 (129).

[14] *Eisenmann et al*, Platform Networks – Core Concepts: Executive Summary, MIT Center for Digital Business, Paper 232 (June 2007), p. 11.

provide to the consumer. **Lock-in effects** occur because of the potential loss of the network benefit, when consumers consider as more economically rational to stick with an existing product or service rather than to switch to a competing one. Furthermore, if the **switching costs** of migrating to the superior service are too elevated (due to the existence of factors like service termination penalties, incompatibility with already-purchased complementary goods, or sunk costs), regulators can reduce switching costs by requiring cooperation between rivals (e.g., number portability, access to pricing details and quality of service of competing providers or to information related to other users etc.).

Additionally, the **formation of a network monopoly** will largely depend on competitors' access not to the underlying platform or network and its users, but to the **complementary products**.

Besides the direct competitive strategies, the **competition in R&D** represents a meaningful **strategic alternative**, with several firms competing in R&D even if at that same time there is little direct competition in the product market.

# 3 Digital Transformation and 5G Requirements - Network Slicing and Spectrum Management

## 3.1 Cyber-Physical Systems and the Fourth Industrial Revolution

The Boston Consulting Group (BCG) describes the new wave of hyperconnected industrial technology, branded **Industry 4.0**, as "a transformation that makes it possible to gather and analyse data across machines, enabling faster, more flexible, and more efficient processes to produce higher-quality goods at reduced costs". BCG also identifies **nine technologies that are transforming industrial production** through an improved productivity, a shift of industrial economics, or by supporting industrial growth, and even altering the profile of the labour force – "ultimately changing the competitiveness of companies and regions". The nine **key technologies** are the following: 1.) Big Data and Analytics; 2.) Autonomous Robots; 3.) Simulation; 4.) Horizontal and Vertical System Integration; 5.) The Industrial Internet of Things; 6.) Cybersecurity; 7.) The Cloud; 8.) Additive Manufacturing; and 9.) Augmented Reality.[15]

Most of the buzz-terms like *Internet of Things (IoT)*, *Industry 4.0*, the *Industrial Internet*, *Machine-to-Machine (M2M)* communications, the *Internet of Everything*, *TSensors* (trillion sensors), and *the fog* (similar to the cloud, yet

[15] Boston Consulting Group (BCG), Embracing Industry 4.0 and Rediscovering Growth, 2019.

closer to the ground) are closely linked to the concept of "cyber-physical systems". Lee (2015) defines a **cyber-physical system (CPS)** as "an orchestration of computers and physical systems" in which "embedded computers monitor and control physical processes, usually with feedback loops, where physical processes affect computations and vice versa" - showcasing "a vision of a technology that deeply connects our physical world with our information world".[16]

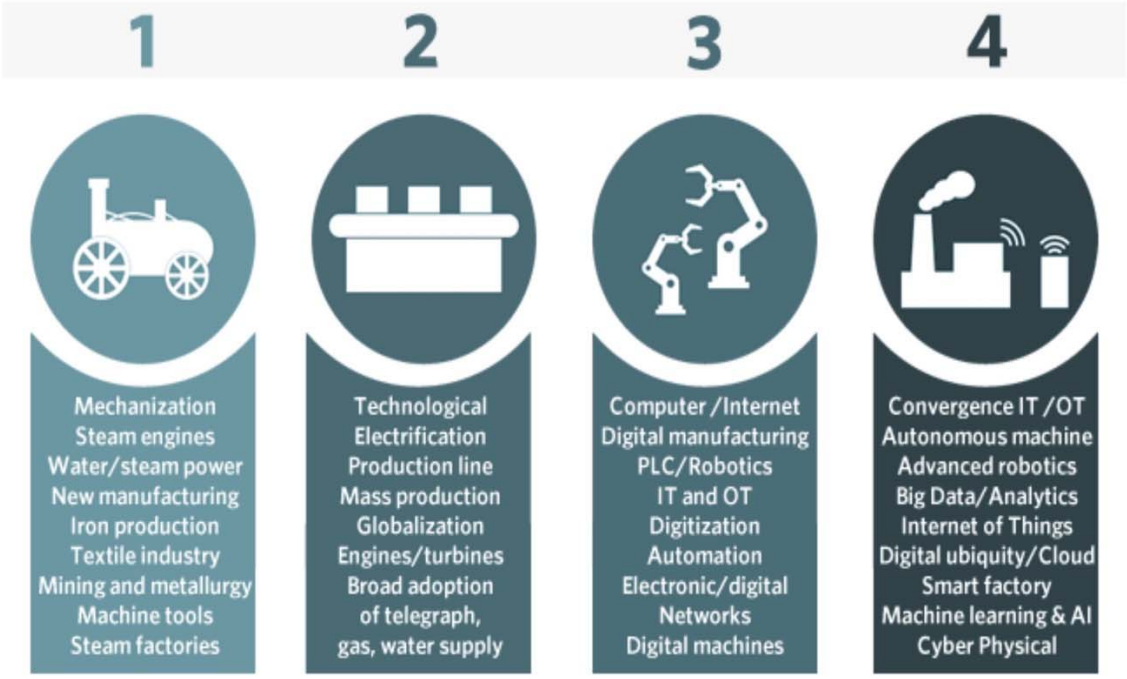


*Fig. 6: Fourth industrial revolution viewpoint of Industry 4.0. Historic perspective. (SOURCE: i-SCOOP)*[17]

Consulting firms like i-SCOOP also link CPS to Industry 4.0 and the **Fourth Industrial Revolution** (see Fig. 6.), as they enable **smart plants**, **smart factories** and anything smart. According to their definition, **Industry 4.0** is "*the digital transformation of manufacturing, leveraging third platform technologies and innovation accelerators in the convergence of IT (Information Technology) and OT (Operational Technology) to realize connected factories and industry, smart decentralized and self-optimizing systems and the digital supply chain in the information-driven cyber-physical environment of the 4th industrial revolution (sometimes called 4IR)*".[18]

---

[16] *Lee*, The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. Sensors 2015, p. 4837 (4869).

[17] i-SCOOP Consulting, Industry 4.0. Available at: https://www.i-scoop.eu/industry-4-0/. (last access: 20.7.2019).

[18] i-SCOOP Consulting, Industry 4.0. Available at: https://www.i-scoop.eu/industry-4-0/. (last access: 20.7.2019).

### 3.2 5G Requirements - Network Slicing and Spectrum Management

According to the Global mobile Suppliers Association (GSA, 2017), 5G digitalization will represent a critical technology in intensifying industrial digitalization, generating and improving **industry digitalization application scenarios** (e.g. immersive gaming, autonomous driving, remote robotic surgery and augmented reality support for maintenance and repair situations).[19]

Other important international organizations like the GSM Association (GSMA) consider that "communication technology has been a catalyst to the digitalisation of society, and a significant contributor to Gross Domestic Product (GDP) growth across the world" - with the perspective of further developing areas that are not presently entirely utilizing the potential of mobile communication services (e.g. financial services, healthcare etc.). The sheer variety, and even the contradictory nature, of communications requirements of such segments are identified as the main source of sub-optimal use of the mobile network. Accordingly, some business users, may necessitate ultra-reliable services, while other business clients may demand ultra-high-bandwidth communication or extremely low latency.[20]

As the global society becomes ever more digitally and globally linked, almost all economic and social sectors are undergoing an ICT-driven transformation. Consequently, the design of the future **5G network** has to be capable to deliver a different mix of capabilities to simultaneously cover all these diverse requirements.

As the Global mobile Suppliers Association (GSA, 2017) emphasises, "**business trends** such as hyper competition, new customer power and sophistication, the fast-paced change in business ecosystems and disruptive technological advances all affect vertical industries to different extents", posing significative challenges to businesses.[21] (See Fig. 7.)

[19] GSA - Global mobile Suppliers Association - Report, 5G Network Slicing for Vertical Indus-tries, 2017, p. 3. Available at: https://gsacom.com/paper/5g-network-slicing-vertic al-industries/. (last access: 20.7.2019).

[20] GSMA Report, An Introduction to Network Slicing, 2017, p. 3. Available at: https://www .gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Ne twork-Slicing.pdf. (last access: 20.7.2019).

[21] GSA - Global mobile Suppliers Association - Report, 5G Network Slicing for Vertical Industries, 2017, p. 3, https://gsacom.com/paper/5g-network-slicing-vertical-industries/ (last access: 20.7.2019).

*Fig. 7: Key Industries and their challenges (SOURCE: GSA, 2017)*

The GSA (2017) examined the different **5G vertical requirements** and elaborated the following **classification**:

a) **Operational Requirements**, (involving: Latency, Throughput, Availability and Resilience/Service always availability, Reliability, Coverage);
b) **Functional Requirements** (concerning: Security and Identity Management; Isolation of the different vertical industries); and
c) **Performance Requirements** (related to: Self-Management of resources/policies, APIs, Service Assurance for core requirement of vertical's business; Charging/ Billing; Global Operation).

Vertical industries are extremely varied, and their requirements are determined by the service features of the related vertical segment (for instance, Autonomous Vehicles, Industrial Control, and Augmented Reality are sectors necessitating Low Latency and High Reliability).

In order to cover such diverse requirements, **flexibility** is one of the key features for 5G networks. As researchers like El Hakim (2019) point out, previous **traditional electronic communications networks** were constructed with **physical nodes** to provide all the services offered by the network operator. While the conventional network was statically configured, predominantly manually managed and designed as a single tenant environment, the introduction of novel 5G networks will move beyond the conventional system into a new ground-breaking, multi-tenant and responsive ecosystem. In this context, the innovative philosophy of **Network Slicing** is one of the most significant 5G technological developments for conveying "customized, dedicated and logically isolated network services based on the differentiated requirements of various vertical industries".[22]

According to GSMA, network slicing represents a total departure from existing network implementations as "with network slicing, the 5G network is able to adapt to the external environment rather than the other way around" and "allows running multiple logical networks as virtually independent business operations on a common physical infrastructure in an efficient and economical way".[23]

The GSA 2017 report highlights that, in contrast to traditional monolithic communications networks, 5G networks will allow the construction of **logical networks** on top of a shared infrastructure (which can be adjusted for specific use cases, service types and support diverse business models - see Fig. 8.). Vital technologies for implementing the concept of "**network as a service**" are virtualization, **Software Defined Networks (SDN)**, orchestration capabilities, improvements in air interface combined with a broad evolution of software technologies.

Furthermore, the GSA explains the advantages of logical networks - which can be designed, instantiated and operated in a dynamic *on-demand* basis, aiming at the particular needs of individual customers, services or business segments, be it related to service characteristics, business models, self-management of resources/service etc.

[22] *El Hakim*, 5G Network Slicing Reference Model, White Paper, 2019, 10.13140/RG.2.2.29 838.82240. Available at: https://www.researchgate.net/publication/ 331904582_5G_Network_Slicing_Reference_Model_White_Paper (last access: 20.7.2019).

[23] GSMA Report, An Introduction to Network Slicing, 2017.

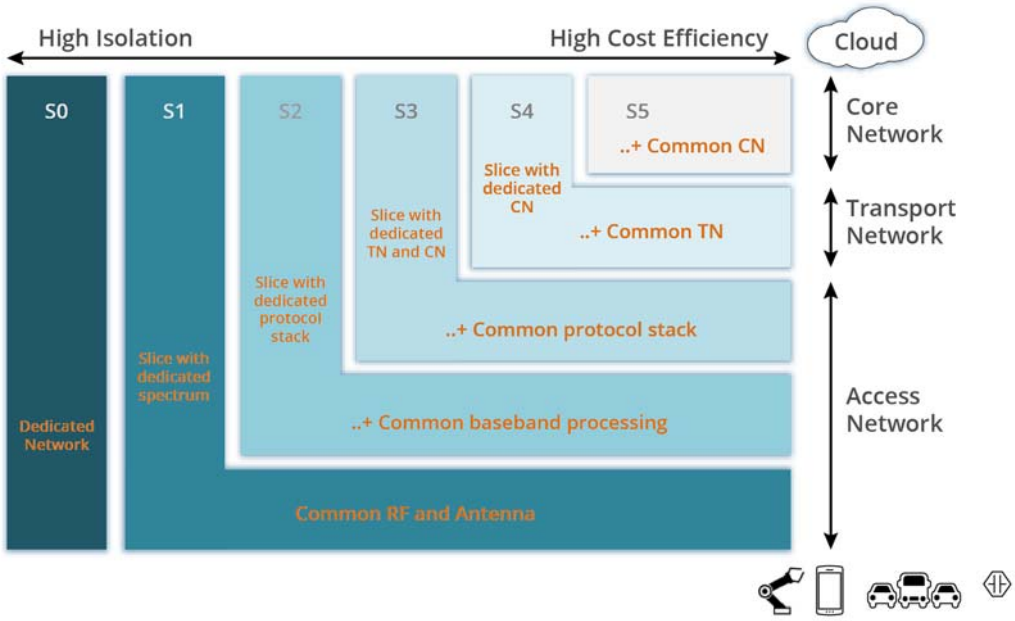


*Fig. 8: Solution to handle diverse vertical requirements (SOURCE: GSA, 2017)*

Logical networks are designated as **Network Slices**, encompassing a logical set of infrastructure resources (i.e., physical, logical, virtual resources) to support functions and services of the network. The GSA considers that a network slice constitutes a "group of network functions, resources and connection relationships, covering multiple technical domains, which includes terminal, access network, transport network, core network, data centre domain that hosts third-party applications, as well as network management system, etc.".[24]

Nicolas Bihannic believes that network slicing should also profit from another disruptive and promising digital technology: the **Blockchain** (due to its characteristics, which are especially appropriate for B2B markets that commonly embrace several partners in the end-to-end value chain of each ecosystem).[25]

Additionally, Weiss et al. (2018) point out that: "Spectrum sharing mechanisms have evolved to meet different needs related to increasing spectrum use efficiency. At first, decentralized and opportunistic cognitive radios (and cognitive radio networks) were the primary focus of research for these

[24] GSA - Global mobile Suppliers Association - Report, 5G Network Slicing for Vertical Industries, 2017, p. 10.

[25] *Bihannic et al*, Network Slicing and Blockchain to Sup-port the Transformation of Connectivity Services in the Manufacturing Industry, IEEE Softwarization, Mar. 2018, https://sdn.ieee.org/newsletter/march-2018/network-slicing-and-blockchain-to-support-the-transformation-of-connectivity-services-in-the-manufacturing-industry (last access: 20.7. 2019).

mechanisms. This gradually transitioned towards the development of co-operative sharing methods based on databases [...]".[26] They consider the Blockchain technology to be a potential catalyst for a dynamic and fine-grained spectrum rights regime constructed on the more efficient **Distributed Ledgers** database management mechanism – in contrast with conventional exclusive frequency allocations.

Weiss et al. (2018) also highlight the benefits of Blockchain - as an effective instrument for spectrum management - which entails advantages compared to centralized databases for recording property rights and assets, especially when information about spectrum access rights and usage can be documented on a *distributed ledger* and managed using *smart contracts* (see Fig. 9).

| Benefit | Potential Application to Spectrum Sharing |
|---|---|
| **Decentralization** | Eliminate the need for trusted third parties such as spectrum licensees, band managers, and database/SAS administrators. |
| **Transparency** | Better localized visibility into spectrum usage; auditability of activity for effective implementation of spectrum sharing rules. |
| **Immutability** | Permanent records prevent tampering, facilitate accurate auditing/enforcement, and can ensure accurate implementation of rules. |
| **Availability** | More reliable accessibility of spectrum sharing databases. |
| **Security** | As communications infrastructure, wireless systems need strong security against attacks. Secure ledgers also foster reliable enforcement of sharing regimes. |

*Fig. 9: Blockchain characteristics applied to spectrum sharing (Weiss et al., 2018)*

## 4 Conclusions

The approach on handling network effects is one of the fundamental issues in digital infrastructure regulation. Network effects - which are inherent to digital platforms and networks - can both trigger monopoly and complicate the management of transitions to proficient competition in 5G electronic communications services, IoT and other digital network markets.

According to GSA - 5G Spectrum Regulation Recommendations, individual national licences are a crucial foundation of the remarkable success of

[26] *Weiss et al*, On the Application of Blockchains to Spectrum Man-agement (July 25, 2018). TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018, p. 4. Available at: https://ssrn.com/abstract=3141910 (last access: 20.7. 2019).

mobile communications services and provide confidence to mobile operators that they can deploy their networks when and where demand arises from their clients.

As with other development stages of the electronic communications networks (from 1G to 4G/LTE), regulation authorities should avert spectrum fragmentation and eschew scarcity and, additionally, licences allocation should be planned to stimulate spectrum usage, maximize benefit for society and not to maximize revenue, while encouraging network investment and deployment. In this context, auctions are a fair award mechanism and can rationally allocate 5G spectrum to those users who value it the most, consequently, supporting the rapid deployment of Industry 4.0.

At the moment, blockchain technologies seem to be a promising solution for a more efficient usage and a dynamic allocation of 5G radio spectrum in the future. Nevertheless, given the incipient phase and the erratic character of development activity and interest in blockchain technology today, blockchain approaches to dynamic 5G spectrum sharing necessitate further investigation.

## References

*Bihannic, Nicolas/Lejkin, Thierry/Finkler, Isabelle/Frerejean, Alexis:* Network Slicing and Blockchain to Sup-port the Transformation of Connectivity Services in the Manufacturing Industry, IEEE Softwariation, Mar. 2018, https://sdn.ieee.org/newsletter/march-2018/network-slicing-an d-blockchain-to-support-the-transformation-of-connectivity-services-i n-the-manufacturing-industry (last access: 20.7.2019).

*Boston Consulting Group (BCG):* Embracing Industry 4.0 and Rediscovering Growth, 2019. Available at: https://www.bcg.com/en-ao/capabilities/op erations/embracing-industry-4.0-rediscovering-growth.aspx (last access: 20.7.2019).

*Crampes, Claude:* Network Industries and Network Goods (Introductory chapter to a study for the European Commission), IDEI, September 1997. Av.: http://idei.fr/sites/default/files/medias/doc/by/crampes/n etwork.pdf (last access: 20.7.2019).

*Economides, Nicholas:* Notes on Network Economics for the MBA class "Networks, Tele-communications Economics, and Digital Convergence", September 2003, http://neconomides.stern.nyu.edu/networks /Net-notes_2003.pdf (last access: 20.7.2019).

*Eisenmann, Thomas/Parker, Geoffrey/Van Alstyne, Marshall:* Platform Networks – Core Concepts: Executive Summary, MIT Center for Digital Business, Paper 232 (June 2007), http://ebusiness.mit.edu/research/p apers/232_VanAlstyne_NW_as_Platform.pdf (last access: 20.7.2019).

*El Hakim, Ahmed:* 5G Network Slicing Reference Model, White Paper, 2019, 10.13140/RG.2.2.29838.82240, https://www.researchgate.net/ publication/331904582_5G_Network_Slicing_Reference_Model_Whit e_Paper (last access: 20.7.2019).

*Energy Policy Research Group:* Electricity markets as platform markets, 2014, http://www.eprg.group.cam.ac.uk/wp-content/uploads/2013/10/Slid es-for-EPRG-meeting.pptx (last access: 20.7.2019).

*GSA - Global mobile Suppliers Association – Report*: 5G Network Slicing for Vertical Industries, 2017, https://gsacom.com/paper/5g-network-slicing-vertica l-industries/ (last access: 20.7.2019).

*GSMA Report:* An Introduction to Network Slicing, 2017, https://www.gsma.c om/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introdu ction-to-Network-Slicing.pdf (last access: 20.7.2019).

*Hagiu, Andrei/Wright, Julian:* Multi-Sided Platforms, in International Journal of Industrial Organization 43 (November 2015): 162–174. https:// www.hbs.edu/faculty/Pages/item.aspx?num=49004 (last access: 20.7. 2019).

*i-SCOOP Consulting:* Available at: https://www.i-scoop.eu/industry-4-0/.

*Lee, Edward A.:* The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. Sensors, 2015, 4837-4869, https://www.mdpi.com/1424-8220/15/3/4837/pdf (last access: 20.7.2019).

*Martens, Bertin:* An Economic Policy Perspective on Online Platforms, Institute for Prospective Technological Studies Digital Economy Working Paper 2016/05. JRC101501, https://ec.europa.eu/jrc/sites/jrcsh/files/JRC101501.pdf (last access: 20.7.2019).

*Metcalfe, Bob:* Metcalfe's law after 40 years of Ethernet, 2013, IEEE Computer. 46 (12), pp. 26–31.

*Rysman, Marc:* The Economics of Two-Sided Markets, Journal of Economic Perspectives, 2009, pp. 125-43, https://EconPapers.repec.org/RePEc:aea:jecper:v:23:y:2009:i:3:p:125-43 (last access: 20.7.2019).

*Weiller, Claire M./Pollitt, Michael G.:* Platform Markets and Energy Services, Cam-bridge Working Papers in Economics 1361, Faculty of Economics, University of Cam-bridge, 2013, https://www.eprg.group.cam.ac.uk/wp-content/uploads/2013/12/1334-PDF.pdf (last access: 20.7.2019).

*Weiser, Phil:* Network Economics 101, Aspen, Colorado, April 29, 2007, http://www.pff.org/issues-pubs/testimony/2007/070430IRLE2007networkeconomics101.ppt (last access: 20.7.2019).

*Weiss, Martin B.H./Werbach, Kevin/Sicker, Douglas/Caicedo, Carlos/Malki, Amer:* On the Application of Blockchains to Spectrum Management (July 25, 2018), in TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018, https://ssrn.com/abstract=3141910 (last access: 20.7.2019).

# EUROPÄISCHE STAATSANWALTSCHAFT: EIN EFFEKTIVES INSTRUMENT ZUR BEKÄMPFUNG DER COMPUTERKRIMINALITÄT?

PD Dr. Irini Vassilaki

Rechtsanwältin: ivassilaki@vassilaki.net

## Zusammenfassung

Computerkriminalität ist ein transnationales Phänomen. Während das materielle Strafrecht den größten Teil dieser Aktivitäten erfassen kann, erscheint ihre Strafverfolgung oft als Hindernis. Eine Lösung dieses Problems könnte die Strafverfolgung durch die EuStA anbieten. Obwohl in diesem Zeitpunkt diese Institution keine Kompetenz für die Strafverfolgung der Computerkriminalität hat, könnte ihr durch eine Kompetenzerweiterung eine solche Option erteilt werden. Die EuStA sollte nur für internationale Sachverhalte eingesetzt werde, die sonst nicht gelöst werden können. Die Anwendung in diesem Fall des Subsidiaritätsprinzips fördert die Entwicklung eines gerechten internationalen Wertentscheidungssystems.

## 1 Problemstellung

Das Internet, das globale Cyberspace und die Nutzung von Social Media unterstützen die Entstehung einer „Weltgesellschaft", die kein neues Phänomen darstellt. Schon die antiken Großreichen bildeten über das Nationale hinausreichende Kommunikations- Handels- und Rechtsräume. Die technischen Entwicklungen verwandeln diesen Begriff zu einer „Welt-Informationsgesellschaft".[1] Die Vernetzung der Welt-Informationsgesellschaft verdeutlichen, die Risiken und Gefahren, die der technische Fortschritt mit sich bringt. Dies wurde von dem neulich begangenen Diebstahl persönlicher Daten hunderter deutscher Politiker und Prominenter bewiesen.

Dezentralisierte Dienste, wie das Cloud-Computing, grenzüberschreitende Kommunikation und Mobilität von Menschen und Unternehmen erschweren die Bestrafung von Delikten, die mit der Informationsgesellschaft verbunden sind. Dazu kommt – hauptsächlich - das Fehlen von kriminologischen Studien zu den einschlägigen Phänomenen, die Komplexität der neugefügten computerbezogenen Strafvorschriften und der Mangel an einer umfassenden Strafrechtsreform. Denn die bestehenden Strafnormen wurden meistens für körperliche Gegenstände entwickelt. Es besteht auch

[1] Dazu siehe *Sieber*, Rechtliche Ordnung in einer globalen Welt, S. 152.

keine Einigkeit in Bezug auf die kriminologische bzw. strafrechtliche Beschreibung, Eingrenzung und Benennung der Kriminalitätsformen, die mit der Informationstechnik in irgendeiner Weise verbunden sind.[2] Wissenschaft und Praxis verwendet oft unterschiedliche Begriffe, wie Internetkriminalität, Cyberkriminalität, Hightechkriminalität und Multimediale Kriminalität.[3] Im Folgenden werde ich den Begriff „Computerkriminalität" verwenden, weil dieser Begriff historisch als Ausgangspunkt (engl.: computer crime und computer-related crime) der Begriffsdebatte gesehen werden kann und weil er in Art. 83 Abs. 1 UAbs. 2 AEUV verankert ist.

## 2 Bestrafung der transnationalen Computerkriminalität

### 2.1 Materielles internationales Strafrecht vs. Strafverfolgung

Das Hauptproblem der Bestrafung der Computerkriminalität liegt darin, dass aus vielen Sachverhalten, sich Fragen des internationalen Strafrechts ergeben und dass die Eingriffsbefugnisse der Strafverfolgungsbehörden der digitalen Welt angepasst werden sollen. Aus den transnationalen Sachverhalten ergeben sich immer häufiger grenzüberschreitende Rechtsfragen.[4]

Auf internationaler Ebene können die entstehenden Probleme des transnationalen materiellen Strafrechts entweder mit der Anwendung der Strafvorschriften der nationalen Strafgesetzbücher oder mit der Umsetzung von supranationalen Texten, etwa der Cybercrime-Konvention des Europarats, der Richtlinie 2011/93/EU30 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie oder der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme, oft bewältigt werden. Die Frage der Durchsetzung des materiellen Strafrechts, wenn es sich um transnationale Sachverhalte handelt, bleibt allerdings offen. Grenzüberschreitende Strafverfolgungsmaßnahmen zu koordinieren und auf Personen oder Beweismitteln im Ausland zuzugreifen, ist für das Strafverfahren eine Herausforderung.

Zwei sind dabei die wichtigsten Gründe, die die effektive Computerkriminalitätsbekämpfung auf internationaler Ebene erschweren:

a) Mangelnde Ermittlungsmöglichkeiten der Polizei und der Strafverfolgungsbehörden in Verbindung mit langer behördlicher Reaktionszeit bei transnationalen Sachverhalten.

---

[2] Siehe dazu *Sieber*, Straftaten und Strafverfolgung im Internet, C 9 ff.

[3] Über die unterschiedlichen Definitionen siehe UN, Comprehensive Study on Cybercrime, S. 11 f.; ausführlich auch *Haase*, Computerkriminalität, S. 61 ff.

[4] Dazu auch UN, Comprehensive Study on Cybercrime, S. 183 ff.

b) Doppelbestrafungsausschluss: Um zu verhindern, dass Straftäter bei transnationalen Delikten in sämtlichen berührten Rechtsordnungen verurteilt werden, gibt es in der EU durch Art. 50 GRC sowie Art. 54 SDÜ einen Doppelbestrafungsausschluss.[5] Oft aus Kostengründen vertrauen die nationalen Behörden, dass die Strafverfolgungsbehörden anderer Mitgliedstaaten tätig werden und ermitteln selbstständig nicht. Dies hat als Folge, dass der EU-Doppelbestrafungsausschluss teilweise dazu führt, dass letztlich überhaupt kein Mitgliedstaat die Strafverfolgung übernimmt.[6]

Daher wird die Durchsetzungsmacht des Nationalstaates in einem „race to the bottom" eingeschränkt.[7] Wichtige Aufgabe des Rechts in der Welt-Informationsgesellschaft besteht demzufolge darin, die Geltung und Durchsetzung der Rechtsnormen auch transnational zu gewährleisten.

### 2.2 Strafverfolgung durch die EuStA?

Eine Lösung könnte die Kompetenzausweitung der Europäischen Staatsanwaltschaft gewähren.

Im November 2017 hat die EU die Verordnung (EU) Nr. 2017/1939 zur Errichtung der Europäischen Staatsanwaltschaft (EuStA) angenommen. Nach Art. 4 der Verordnung, ist die EuStA zuständig für die strafrechtliche Untersuchung und Verfolgung sowie die Anklageerhebung in Bezug auf Personen, die als Täter oder Teilnehmer Straftaten zum Nachteil der finanziellen Interessen der Union, die in der Richtlinie (EU) 2017/1371 vorgesehen und in dieser Verordnung bestimmt sind, begangen haben. Diese EU-weit tätige Behörde wird nur gegen grenzübergreifende Großkriminalität zu Lasten des EU-Haushalts vorgehen.

Damit scheidet zunächst die Computerkriminalität aus dem Kompetenzbereich der EuStA aus. Es stellt sich aber die Frage, ob und unter welchen Voraussetzungen diese Kriminalitätsform eine Rechtsmaterie darstellt, die geeignet für eine Zuständigkeitserweiterung der EuStA ist.

### 2.3 Kompetenzerweiterung der EuStA

Die Antwort befindet sich in Art. 86 Abs. 4 AEUV,[8] der festlegt, dass durch einen Beschluss des Europäischen Rates die Kompetenz der EuStA, die auf

---

[5] Dazu auch *Brodowski*, ZIS 2017, S. 11(12).

[6] *Brodowski*, in: Lange/Bötticher, Cyber-Sicherheit, S. 249 (259).

[7] Dieser Begriff, (Unterbietungswettlauf), den zum ersten Mal von William Cary im Jahr 1974 in einem Aufsatz verwendet hatte, wo er die neue Unternehmensgesetzgebung des Staates Delaware kritisierte, beschreibt den stetigen Abbau von Standards insb. im Sozial-, Arbeits-, Umweltrecht im globalisierten Wettbewerb und internationalen Steuerwettbewerb; siehe *Cary*, Yale L.J. 1974, S. 663 (705).

[8] Zum Art. 86 AEUV siehe auch *Krüger*, HRRS 2012, S. 311 (317).

die Bekämpfung von Straftaten zum Nachteil der finanziellen Interessen der Union begrenzt ist, auf die Bekämpfung der schweren Kriminalität mit grenzüberschreitender Dimension erweitert werden kann.[9]

Im Anschluss daran, normiert Art. 83 Abs. 1 UAbs. 1 und 2 AEUV, dass: "das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität festlegen können, die aufgrund der Art oder der Auswirkungen der Straftaten oder aufgrund einer besonderen Notwendigkeit, sie auf einer gemeinsamen Grundlage zu bekämpfen, eine grenzüberschreitende Dimension haben. Derartige Kriminalitätsbereiche sind: Terrorismus, Menschenhandel und sexuelle Ausbeutung von Frauen und Kindern, illegaler Drogenhandel, illegaler Waffenhandel, Geldwäsche, Korruption, Fälschung von Zahlungsmitteln, Computerkriminalität und organisierte Kriminalität." Demzufolge erfasst die Erweiterungsmöglichkeit des Art. 86 Abs. 4 AEUV auch die Computerkriminalität.[10]

### 2.4 Ermittlungs- und Beweiserhebungsbefugnisse der EuStA

Sollte nunmehr der Zuständigkeitsbereich der EuStA auch die Bekämpfung der Computerkriminalität erfassen, stellt sich die Frage, in welcher Weise diese europäische Behörde tätig würde. Einerseits wäre zu klären, welche strafprozessualen Ermittlungs- und Beweiserhebungsbefugnisse der neuen EU-Behörde zufielen. Da die Ermittlungen im Bereich der Computerkriminalität Besonderheiten gegenüber klassischen Deliktskategorien aufweisen, ist notwendig, dass die Ermittlungsmaßnahmen der digitalen Welt angepasst werden. Als Beispiel seien folgende Ermittlungsmaßnahmen erwähnt:

- Die Online-Durchsuchung zu repressiven Zwecken soll beim Verdacht zurückliegender schwerer Straftaten und gleichzeitiger schwerer zukünftiger Gefahren ermöglicht werden.
- Die Abgrenzung zwischen der Telekommunikationsüberwachung und der Durchsuchung soll klargestellt werden. Insbesondere soll betont werden, dass die besonders eingriffsintensiven heimlichen und permanenten Maßnahmen nur unter den strengeren Voraussetzungen der Telekommunikationsüberwachung möglich sind.
- Die Prämissen sollen festgelegt werden, die Auskunftspflichten gegenüber dem Staatsanwalt und dem Richter über Zugriffs- und Entschlüs-

[9] Ausführlich dazu: *Rheinbay*, Die Errichtung einer Europäischen Staatsanwaltschaft, S. 113 ff.

[10] H.M. siehe dazu etwa *Dannecker*, in: Streinz (Hrsg.), Art. 86 AEUV Rn. 6.

selungscodes normieren. Insbesondere soll klargestellt werden, dass dafür strengere Voraussetzungen als für die allgemeinen Auskunftspflichten gelten werden.

- Die strafprozessualen Herausgabepflichten für Nicht-Beschuldigte und die informatikspezifischen Pflichten zur Herausgabe spezifizierter Dateninhalte und Datenformate, zu denen im Rahmen des Möglichen auch die Verpflichtung zur Entschlüsselung von Daten zählt, sollen festgelegt werden.
- Es soll geregelt werden, unter welchen Voraussetzungen das Abhören der Daten an den noch unverschlüsselten Schnittstellen der Endgeräte – nämlich die Quelldatentelekommunikationsüberwachung - erlaubt ist.
- Der Zugriff auf Verkehrsdaten muss geregelt werden. Für die spezielle Zuordnung von dynamischen IP-Adressen zu ihren Anschlussinhabern soll ebenso wie für den Zugriff auf Bestandsdaten die Möglichkeit eines automatisierten Auskunftsverfahrens in Echtzeit geschaffen werden.
- Das „Quick-Freeze-Verfahren“ soll nicht nur für Verkehrsdaten, sondern – wie von der Cybercrime-Konvention des Europarats gefordert – für alle Datenbestände eingeführt werden. Die Ermittlungsbehörden müssen demzufolge bei Gefahr des Datenverlusts kurzfristig und ohne richterliche Entscheidung die Sicherung der Daten verlangen können, die von den Adressaten erst nach einer richterlichen Entscheidung herauszugeben sind.[11]

### 2.5 Ausschließliche oder ergänzende Strafverfolgungskompetenz der EuStA?

Weiterhin soll geregelt werden, ob der EuStA im Bereich der Computerkriminalität ausschließlicher Strafverfolgungskompetenz zufällt oder ob sie ergänzend zu den mitgliedstaatlichen Staatsanwaltschaften tätig wird.

Art. 86 Abs. 4 S. 1 AEUV setzt für die Ausdehnung der Befugnisse der Europäischen Staatsanwaltschaft auf die Bekämpfung der schweren Kriminalität mit grenzüberschreitender Dimension das Vorliegen von Straftaten voraus, die sich auf mindestens zwei Mitgliedstaaten beziehen. Nationale Sachverhaltskonstellationen können nicht in den Zuständigkeitsbereich der EuStA fallen. Demzufolge ist zu entscheiden, ob beim Vorliegen transnationaler Sachverhalte ausschließliche oder lediglich eine zusätzliche/komplementäre Strafverfolgungszuständigkeit auf die EuStA übergehen sollte. Weil die Beauftragung der EuStA mit sämtlichen Computerdelikten die neue Behörde überfordern wurde und Parallelstrukturen von nationalen

[11] Ausführlich dazu siehe *Sieber*, Straftaten und Strafverfolgung im Internet, C103 ff.; UN, Comprehensive Study on Cybercrime, S. 127 ff., 157 ff.

und internationalen Strafverfolgungsbehörden nicht geeignet seien, strukturelle Defizite zu beheben, ist der zusätzlichen/komplementären Strafverfolgungszuständigkeit den Vorzug zu geben. Außerdem, da bei Computerstraftaten meistens um Massenkriminalität handelt, lässt sich diese mit einer komplementären Infrastruktur der EuStA sinnvoll bewältigen. Außerdem sind die Mitgliedstaaten bei der Computerkriminalität immer auch selbst an einer Aufklärung interessiert.[12]

### 2.6 „Entstaatlichung" des Rechts?

Wichtiger Grund, der für die komplementäre Zuständigkeit der EuStA spricht, liegt außerdem darin, dass der Nationalstaat die umfassende raumgebundene rechtliche Herrschaftsmacht über seine Staatsbürger nicht verlieren darf, indem die Staatsgewalt durch andere internationale Gewalten überlagert wird.

Man darf nicht vergessen, dass die Legitimation für die Einführung von Regelungen eines supranationalen Strafverfolgungsmodells außerhalb des Nationalstaates liegt. Die im demokratischen, parlamentarischen Nationalstaat entwickelten Grundsätze der Gewaltteilung, Menschenrechte und des Rechtschutzes haben in der Welt-Informationsgesellschaft nur begrenzte Wirkung. Dies spielt insbesondere im Bereich des Strafrechts eine wichtige Rolle, wo der Grundsatz „nullum crimen sine lege parlamentaria" zentrale Bedeutung hat.

Die Bekämpfung/Strafverfolgung der Computerkriminalität durch die EuStA stellt ein Beispiel für den Wandel der „Staatlichkeit" im 21. Jahrhundert dar. Die Vorherrschaft des Staates gegenüber anderen Organisationsformen, wie die Europäische Union, wird schwächer. Die Dominanz des Nationalstaates bei der Schaffung Rechtsrahmen stellt sich in Frage. Die internationalen und supranationalen Regelungen werden nicht mehr von Parlamenten, sondern von anderen Akteuren beherrscht. Die Normen werden hauptsächlich von Bürokraten der internationalen Institutionen, von Lobbyisten und Vertretern der wirtschaftlich starken Staaten entworfen und durchgesetzt. Die „Entstaatlichung" des Rechts ist im vollen Gange.[13]

Die „Entstaatlichung" des Rechts insbesondere des Straf- und Strafprozessrechts muss Grenzen haben. Wegen der Schärfe der Konsequenzen ihrer Regelungen dürfen die Nationalstaaten ihre Souveränitätsrechte nicht aufgeben. In diesem Bereich soll das Subsidiaritätsprinzip gelten bleiben. Dies kann verwirklicht werden, indem supranationale Institutionen, wie die EuStA, für internationale Sachverhalte eingesetzt werde, die sonst nicht

[12] Ausführlich dazu *Haase*, Computerkriminalität, S. 235 ff.

[13] Über die „Entstaatlichung" des Rechts siehe *Sieber*, Rechtliche Ordnung in einer globalen Welt, S. 169 f.

gelöst werden können. Diese Lösung ist die einzige, die Fragen des Menschenrechtsschutzes und der Legitimationsproblematik gerecht wird. Hinzu kann sie die Entwicklung eines gerechten internationalen Wertentscheidungssystems fördern und die Entstehung eines ungerechten rechtlichen Weltföderationssystems verhindern.

## 3 Fazit

Die Bestrafung des transnationalen Computerkriminalität stellt nicht nur eine Herausforderung für das internationale Straf- und Strafprozessrecht dar. Themen hinsichtlich der Kompetenzerweiterung der EuStA, wie weit ihre Ermittlungs- und Beweiserhebungsbefugnisse gehen sollen und ob das Subsidiaritätsprinzip Anwendung finden wird, können die Entwicklung eines globalisierten Rechts beeinflussen und dieses zu einem gerechten Rechtsdurchsetzungssystems formieren.

## Literatur

*Brodowski, Dominik:* Cybersicherheit durch Cyber-Strafrecht. Über die strafrechtliche Regulierung des Internets, in: Hans-Jürgen Lange/Astrid Bötticher (Hrsg.), Cyber-Sicherheit, Wiesbaden 2015, S. 249–275.

*Brodowski, Dominik:* Strafrechtsrelevante Entwicklungen in der Europäischen Union – ein Überblick, ZIS 2017, S. 11-27.

*Cary I., William:* Federalism and Corporate Law: Reflections Upon Delaware, Yale Law Journal 1974, S. 663-705.

*Haase, Adrian:* Computerkriminalität im Europäischen Strafrecht – Kompetenzverteilung, Harmonisierungen und Kooperationsperspektiven, Tübingen 2017.

*Krüger, Matthias:* Unmittelbare EU-Strafkompetenzen aus Sicht des deutschen Strafrechts, HRRS 2012, S. 311-317.

*Rheinbay, Susanne:* Die Errichtung einer Europäischen Staatsanwaltschaft, Berlin 2014.

*Sieber, Ulrich:* Verhandlungen des 69. Deutschen Juristentages, München 2012, Bd. I: Gutachten/Teil C: Straftaten und Strafverfolgung im Internet, München 2012.

*Sieber, Ulrich:* Rechtliche Ordnung in einer globalen Welt. Die Entwicklung zu einem fragmentierten System von nationalen, internationalen und privaten Normen, Rechtstheorie 2010, S. 151-198.

*Streinz, Rodulf (Hrsg.):* EUV/AEUV/GRCh – Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrechte der Europäischen Union, Dritter Teil, Teil Fünf, Kap. 4, 3. Aufl. München 2018.

*United Nations:* Comprehensive Study on Cybercrime, Vienna 2013.

# BLOCKCHAIN LEGAL TRENDS

Cristiana Fernbach/Cătălina Fînaru

KPMG Legal – Toncescu si Asociatii SPRL
cfernbach@kpmg.com, catalinafinaru@kpmg.com

## Summary

Being a type of distributed ledger technology and at the heart of cryptocurrency, blockchain technology is more and more present nowadays. As a promoter in technology development, blockchain technology contributes to the technological development of a range of industries, including banking, insurance or transport industry.

As the most well-known blockchain application, cryptocurrency is an ardent topic at European level. Given the fact that have been issued varied points of view on the cryptocurrency's legal qualification, there is no unanimous legal framework and the European Member States are in the process of adapting to the challenges of the new technology.

## 1 Blockchain – the process behind it

As a digital record system, blockchain is a complex technology, which involves digital information stored in a public database, whereas digital information represents the block and public database represents the chain. The blockchain consists of multiple blocks strung together. In the moment a block stores new data, it is added to the blockchain.

Each block on the blockchain is made up of pieces of information and may be seen as three interconnected parts:

1. block stores information like the date and time about a specific action (e.g. transaction);
2. block stores information about the participant to the specific action in a form of a unique digital identifier;
3. block stores a unique hash code that distinguishes it from other blocks.

Assuming that the information stored in a block refer to a transaction, for a block being added to the blockchain, four steps are carried out. In order to have a clear type of action, we further refer to an online purchasing which have the characteristics of an usual transaction. Therefore:

1. transaction occurs;
2. the transaction is verified – the transaction is verified by a network of computers which confirms the details of the purchase;
3. the transaction is stored in a block – after the transaction has been verified as accurate, the information about the transaction is stored in a block;

4. the block is hashed – once the transaction has been verified, the block must be given a unique hash code. The hashed block is added to the blockchain and in this way it becomes publicly available.

As recognized by the tech industry, the blockchain technology's goal is to allow digital information to be recorded and distributed in a non-editable form.

One of the most known application of blockchain is cryptocurrency technology, which protocol in most cases is built on blockchain. As the use of cryptocurrency is not yet regulated, the transactions made in cryptocurrencies are verified by a network of computers, whereas the users of the network solve a complex mathematical algorithm for the purpose of verification. The completed transaction is publicly recorded and stored as a block on the blockchain and the information becomes unalterable. In the case of the most blockchains applications, the users of the network of computers (also known as miners) that successfully verify blocks are rewarded with cryptocurrency.[1]

## 2 Electronic money vs. virtual currency

Although European legislation do not regulates in a special law a definition of cryptocurrency, the Fifth Money Laundering Directive (Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU) defines virtual coins (cryptocurrency). Consequently, cryptocurrencies are digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

By contrast with cryptocurrencies, there are fiat currencies as coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country. Despite of being a type of fiat currency, electronic money (e-money) is defined in a special European normative act, Directive 2009/110 on the taking up, pursuit and prudential supervision of the business of electronic money institutions. Therefore, e-money means electronically, including magnetically,

[1] Investopedia, Blockchain, Explained, 25.6.2019, https://www.investopedia.com/terms/b/blockchain.asp (last access: 22.7.2019).

stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment and which is accepted by a natural or legal person other than the electronic money issuer.

For a better understanding of the differences between the cryptocurrency and the fiat currency, it is necessary to shortly present them comparatively:

| Cryptocurrency | Fiat currency |
|---|---|
| Created by the computers | Issued by the government |
| Limited supply | Unlimited supply |
| Digital way of money exchange | Physical or electronic way of money exchange |
| Decentralized and not controlled by any entity or government | Centralizes and controlled by the law and banks |
| Its value is not determined by supply and demand | Its value is determined by markets and regulations |
| Not regulated by European and Romanian law | Regulated by European and Romanian law |

Although cryptocurrency may frequently be used as a means of payment, it could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. Consequently, cryptocurrency shall not to be confused with electronic money.

## 3 Legal qualification

European authorities and European Member States authorities have been issued varied points of view on the cryptocurrency legal qualification and there is no unitary approach to the legal qualification. Therefore, cryptocurrency is not considered as being fiat currencies, but is considered as means of exchange rather than as legal means of payment. The consequence of not being recognized as a legal means of payment is that there is no obligation to accept the cryptocurrency payment. Cryptocurrency is considered as being intangible, or as being contractual means of payment or as alternative investment with specific risks, being inherently associated with

the investment risks specific to the financial and banking sector. Some legislations recognized cryptocurrency as being unit of account and, as a consequence, is financial instrument.[2]

Although there is no general regulation of cryptocurrency and its use, the circulation of cryptocurrency is allowed, although in many European Member States the supervisory authorities of the financial sector and/or the central banks have been constantly issued warnings, informing about the absence of any kind of regulation or supervision or about the risks involved in the operation of cryptocurrency and the fact that cryptocurrency does not have a well-defined and accepted legal status at the European level.[3]

## 4 European regulation

Although in most European Member States, regulators and supervisor authorities do not recognize cryptocurrency as a legal means of payment, the use of it is not explicitly forbidden.

Until now, three European Member States have been adopted, even partially, specific legislation on the use of cryptocurrency:

- France;
- Malta;
- Gibraltar.

On the other hand, in countries such as Austria, Latvia, Ireland, Spain and Netherlands, reflections are made on the opportunity to initiate specific normative acts to regulate the use of cryptocurrency. An opposite approach may be identified in several other European Member States that impose certain restrictions on the use of cryptocurrency. Thus, in Belgium, professional commercialization of financial products whose payment depends directly or indirectly on a cryptocurrency is forbidden.[4]

In addition, several European Member States, including the Czech Republic, Croatia, Estonia, France, Latvia, Malta, Poland, Slovenia, Spain etc.,

---

[2] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, page 9.

[3] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, page 9.

[4] Arrêté royal du 24 avril 2014 portant approbation du règlement de l'Autorité des services et marchés financiers concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, at: https://www.fsma.be/sites/default/files/public/sitecore/media%20library/Files/fsmafiles/wetgeving/reglem/reglem_24-04-2014.pdf. (last access: 22.7.2019)

subject or intend to subject the activities related to the cryptocurrency to anti-money laundering and terrorist financing legislation. It is worth to mention that this is also the direction imprinted at European level by the Fifth Money Laundering Directive. Thus, in the recitals to mentioned normative act it is noted that *„terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. For the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT), competent authorities should be able, through obliged entities, to monitor the use of virtual currencies. Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship"*.[5]

## 5 "Mediterranean seven"

Despite the legislative efforts of several European Member States, such as Malta, most of Europe's regional cryptocurrency markets are still significantly weaker compared with Asia and the United States.

In order to emphasize the value of blockchain technology, especially its potential to improve governance and the delivery of public services but also to solve key problems and inefficiencies across many industries, Malta initiated Mediterranean Seven declaration which was signed by six other member states including Cyprus, France, Greece, Italy, Portugal and Spain.

Being quite persistent with its blockchain development endeavours and with its progressive position on blockchain technology, it is no coincidence that Malta initiated the Mediterranean Seven declaration.

The Mediterranean Seven declaration was initiated on December 4th, 2018, after the G20 Summit and its main scope is improving education and spur usage of blockchain technology in the areas of healthcare, transport, land and company registry, education and shipping.

By using smart contracts in areas such as certifying product origin, education, transport, mobility and shipping in order to transform the way that such services are delivered, the blockchain technology is seen as a potential

[5] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, pages 5-6.

game changer. This can lead not only to enhancement of e-government services but also to increase transparency and reduce administrative burdens, better customs collection and better access to public information.[6]

The general perspective stated on the declaration is that *„any legislation on blockchain technologies should take into account the decentralized nature of such technology and should be based on European fundamental principles and technological neutrality. It should also allow innovation and experimentations in order for the public and private sector to better understand the blockchain technologies and to develop use-cases“*.[7]

## 6 National perspective

### 6.1 Austria

Austrian law and National Bank of Austria do not consider cryptocurrency as a fiat currency because it does not fulfil the typical money functions, especially as the supply is unlimited and it is no central authority to support and supervise it. Currently, cryptocurrency is not subject to the Austrian legislation on electronic money or to the Austrian legislation on payment services.

The Financial Market Authority in Austria has been issued many warnings about the lack of regulation and supervision of cryptocurrency and trading platforms and. The Financial Market Authority in Austria does not qualify cryptocurrency as a legal means of payment. However, with regard to initial coin offering (“ICO”), on a case-by-case basis, it is decided whether an ICO may be authorized. The same view is shared by Austrian Ministry of Finance which does not recognize cryptocurrency as a legal means of payment or as a financial instrument. Instead, this authority qualifies cryptocurrency as other incorporeal good and the mining activity as a commercial activity. Therefore, the mining activity is treated like any other production of goods.[8]

### 6.2 Belgium

Although Belgian law does not regulate the use of cryptocurrency, it is defined as any form of unregulated digital currency that has no legal exchange

---

[6] *Walters*, investinblockchain.com 7.12.2018, https://www.investinblockchain.com/eu-mediterranean-seven/ (last access: 22.7.2019).

[7] Southern European Countries Ministerial Declaration on Distributed Ledger Technologies, Declaration of 4.12.2018, https://www.mise.gov.it/images/stories/documenti/Dichiarazione%20MED7%20versione%20in%20inglese.pdf (last access: 22.7.2019).

[8] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, page 20.

rate. Thereby, the professional commercialization of financial products whose payment depends directly or indirectly on a cryptocurrency is prohibited by Belgian legislation.[9]

National Bank of Belgium and other Belgian financial authorities have been issued several warnings about the risks of use of cryptocurrency, given the fact that cryptocurrency is neither a legal means of payment nor a form of fiat money and it is no financial control or supervision of cryptocurrency.

Amongst the identified risks may be find:

- the possibility of piracy of the trading platform or of the electronic wallet;
- the absence of an official assessment of a supervisory authority;
- the fluctuation in the exchange rate for the cryptocurrency may lead to significant financial losses;
- the absence of control of the cryptocurrency exchange rate;
- the absence of a legal guarantee of the possibility of direct change to its initial value;
- the cryptocurrency is not a legal means of payment and there is no obligation to accept the cryptocurrency payment;[10]

### 6.3 France

Under current French legislation, cryptocurrency is not considered as payment instrument nor electronic money or financial instrument. The adaptation of the French legislation on the use of cryptocurrency was made in December 2017 by recognizing for the transfer of financial titles in a blockchain the same legal effects as a book-entry of financial titles.

At the end of 2018, the National Assembly issued a report which included 20 proposed issues to be considered by in legislative process regarding blockchain technology.[11] Among these, the most important proposals refer to:

---

[9] Arrêté royal du 24 avril 2014 portant approbation du règlement de l'Autorité des services et marchés financiers concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail, at: https://www.fsma.be/sites/default/files/public/sitecore/media%20library/Files/fsmafiles/wetgeving/reglem/reglem_24-04-2014.pdf. (last access: 22.7.2019).

[10] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, page 21.

[11] Rapport d'information déposé en application de l'article 145 du Règlement par la mission d'information commune sur les chaînes de blocs (blockchains), http://www.assemb leenationale.fr/15/pdf/rap-info/i1501.pdf (last access: 22.7.2019).

- promoting, through French or European initiatives, the development of a publicly funded public blockchain, following the model of artificial intelligence;
- identification of requirements that would condition the development of blockchain technology and regulation of a relevant definition in EU law;
- promoting research in the blockchain industry, in order to improve public services through blockchain use;
- guaranteeing an adequate regulatory framework;
- making a clear distinction between the regulation of financial and banking services and blockchain services;
- studying the possibility of introducing a specific regime of responsibility and of adapting European and national rules in the field of consumer law regarding the use of blockchain technology.

Currently, French legislature is debating the possibility of regulating a legal regime of ICO. Specific regulations include, among other, fundraising through the use of a shared device, in particular through blockchain technology, by issuing digital tokens. It is also envisaged to regulate this funding and investment modalities for innovative enterprises. The main premise is the absence of a clear legal framework, starting from the very different qualification in French and European law of the issued tokens, since most of them do not meet the characteristics of financial titles. The issuance of tokens will be supervised by the Financial Markets Authority of France and will issue a certificate and will examine the whitepapers. Financial Markets Authority of France could require to tokens' issuers to obtain a status as a legal person established or registered in France.[12]

### 6.4 Germany

German legislation qualifies cryptocurrency as unit of account and therefore, it is considered financial instrument, but the use of cryptocurrency does not imply banking activity.

As regard the provision of token brokerage services through online trading platforms, German legislation provides that, in general, entities which provide such services are generally required to obtain a prior authorization from Federal Financial Supervisory Authority of Germany (also known as BaFin).

[12] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, pages 25-29.

Companies involved in ICOs must also assess on a case-by-case basis whether these activities represent financial operations and financial instruments or securities, which may lead to the need to comply with the relevant financial legislation.

Regarding cryptocurrency, Germany has no specific legislation, the competent supervisory authority has qualified cryptocurrency as financial instrument. This does not mean, however, that the use of those instruments as means of payment is, in itself, a banking activity in the sense of banking legislation. Moreover, the online trading platforms are subject to the competent supervisory authority's authorization, being bound by the same rules on anti-money laundering legislation as other financial service providers.[13]

With regard to blockchain technology, there is no specific German legal framework regulating the use blockchain platforms, the current legislature position is aimed at adapting existing legislation to create a framework for the use of blockchain technology which encourage innovation and investments.

### 6.5 Gibraltar

As one of the few states which regulated blockchain technology, Gibraltar has a specific regulatory framework applicable to the blockchain technology and other applications of distributed ledger technology.

Distributed ledger technology is defined as a database where information is recorded and communicated in a consensual and synchronized way within a multi-nodal network and all copies of the database are compliant.

In 2017, the Gibraltar Financial Services Commission adopted a regulatory framework for distributed ledger technology applicable from the beginning of 2018. Therefore, a company operating in and out of Gibraltar by using a blockchain technology to store and transfer value to others shall be authorized by the Financial Services Commission.

Given the need for a flexible legislation, Gibraltar legislative framework includes a set of guiding principles, thus eliminating the potential limitations generated by the existence of concrete rules that could slow technological development. These principles include, among others:

- pursuing honest and upright activities;
- communicating with customers in a loyal and not misleading manner;
- maintaining adequate, financial and non-financial resources;

[13] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, pages 29-30.

- using high standards relating to secured system access;
- using systems for preventing, detecting and communicating the risks of financial crime.[14]

### 6.6 Malta

In 2018, the Maltese legislature adopted three normative acts regulating the ICOs and the cryptocurrency exchange. Thus, blockchain technology is regulated and supervised by Malta Digital Innovation Authority, the competent authority in the field of technological certification and registration of technology service providers. The authority's main mission is to support the development of innovative technology devices and services in Malta by supervising the specific activity realized by blockchain service providers. With regard to innovative technology devices and services, Maltese legislation regulates the methods by which the Authority for Digital Innovation may recognize innovative technology devices and services.

The normative act regulating virtual financial assets establishes the legal framework for ICOs, for cryptocurrency exchange and the legal framework for the provision of certain services related to cryptocurrency. Moreover, the normative act defines the distributed ledger technology as a database system in which is recorded information exchanged in a consensual and synchronized way within a multi-nodal network.

Distributed ledger technology assets are defined as:

- virtual token;
- virtual financial asset;
- electronic money;
- financial instrument.

The legislation establishes the necessity of carrying out an assessment of the distributed ledger technology asset to determine whether they are electronic money, financial instrument, virtual financial asset or cryptocurrency.

The assessment is mandatory to be carried out by:

[14] Distributed Ledger Technology Regulatory Framework, http://www.gfsc.gi/dlt (last access: 22.7.2019); Financial Services (Distributed Ledger Technology Providers) Regulations 2017, http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf. (last access: 22.7.2019); *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, pages 39.

- companies seeking to launch an ICO in or out of Malta;
- companies that have issued blockchain assets abroad but want to do business in or out of Malta;
- any other entities that will trade such assets.

The purpose of the assessment is to determine the nature of blockchain assets in order to determine whether they can be considered virtual financial assets. If the assessment determines the blockchain assets have the nature of a virtual financial asset, the law requires the submission of a white-paper. On the other hand, if the assessment establishes that blockchain assets do not have the nature of a virtual financial asset, it will determine whether the mentioned assets are a financial instrument within the meaning of Markets in Financial Instruments Directive and of the Maltese legislation on investment services. To the extent that the assessment will conclude that the assets do not fall into any of the two previous categories, assets will be qualified as a virtual token and will have value on the trading platform and can not be changed outside such platforms.[15]

### 6.7 Romania

In 2015, the National Bank of Romania ("NBR") issued a warning stating that *„the cryptocurrency is neither an official currency nor a foreign currency and its acceptance of payment is not legally binding"* Moreover, the NBR has consistently stated that it is not in its duties to supervise the cryptocurrency schemes or cryptocurrency use and at European level, cryptocurrencies are subject to anti-money laundering legislation.

In its warnings, NBR exposes the very high volatility and the low degree of security of the cryptocurrencies compared to the currencies issued by the central banks and to regulated electronic money. In other words, NBR states that cryptocurrency is not suitable to be used as a means of payment, but rather as an investment or speculation.[16]

Starting from the judgment of the Court of Justice of the European Union ("CJEU") in Case C-264/14, Skatteverket vs David Hedqvist, with regard to the VAT regime applicable to cryptocurrency operations, with regard to the VAT regime applicable to cryptocurrency operations, *„the supply of services such as those at issue in the main proceedings, which consist of the exchange of traditional currencies for units of cryptocurrency and vice versa, performed in return*

[15] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, pages 35-36.

[16] *Banu/Clem*, Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, page 44.

*for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients, are transactions exempt from VAT*".[17]

Separate from the VAT exemption, since the end of 2018, eliminating the uncertainties surrounding the tax regime for cryptocurrency transfer, the Romanian tax legislation regulates the applicable taxation system. In consequence, income from the cryptocurrency transfer determined as a positive difference between the sale price and the purchase price, including the direct costs of the transaction, are taxed at a rate of 10 % of the income thus determined.

In March 2019, the Ministry of Communications and Information Society initiated consultations with blockchain industry representatives, financial experts and consultants. It further stresses the importance of blockchain use in „*everyday life in the banking sector, transports, energy, insurance, postal services*". It was also emphasized that "*the unique characteristics of the blockchain have the potential to change traditional processes in various industries through high security and decentralized character that cryptography offers, bringing social and economic benefits to countries where it is adopted*."[18]

### 6.8 Switzerland

In Switzerland, using cryptocurrency is not a prohibited activity but there are no Swiss statutes or regulations which are tailor-made to cryptocurrencies or mining of cryptocurrencies. However, mining of cryptocurrencies is permitted and the activity is not subject to particular legal requirements.

Under Swiss law, ICO and trading activities with cryptocurrencies may be subject to anti-money laundering requirements if the activity is considered financial intermediation according to Swiss law. Regarding the mining activity, it does not constitute financial intermediation and the anti-money laundering does not apply.

With regard to anti-money laundering regulations the following are important:

---

[17] ECJ, decision of 22.10.2015, Case C-264/14 (Skatteverket vs David Hedqvist), ECLI:EU:C:2015:718, point 57.

[18] Minister of Communications and Information Society of Romania: press release on the first institutional meeting between Alexandru Petrescu, the Minister of Communications and Information Society and the representatives of the blockchain industry in Romania, comunicatii.gov.ro 19.3.2019, https://www.comunicatii.gov.ro/prima-intalnire-institutionala-intre-alexandru-petrescu-ministrul-comunicatiilor-si-societatii-informationale-si-reprezentantii-industrie-blockchain-din-romania/ (last access: 22.7.2019).

- ICO' – according to Swiss law, ICO constitutes financial intermediation and it is subject to anti-money laundering. However, if the main feature of the token is to provide access to rights to a non-financial application of blockchain technology, ICO is not subject to anti-money laundering regulation, given the fact that the payment functions only constitute a related service;
- Trading activities – depending on the services offered by the relevant company, activities relating to sales and trading may constitute financial intermediation if one of the following applies:
  a) company accepts or holds on deposit cryptocurrencies belonging to third parties;
  b) company assists in the investment of cryptocurrencies;
  c) company assists in the transfer of cryptocurrencies.

Given the fact that making payment with cryptocurrencies is not a regulated activity, there are no specific requirements to be complied when payments are made.

In 2016, Swiss Government announced its strategy on reducing barriers to market entry for fintech businesses. The efforts made by Swiss legislative to promote fintech development is completed by the private initiatives which offer suggestions on blockchain regarding regulatory like creating a system to be used to assess whether a particular cryptocurrency is likely qualify as a security or not.[19]

## 7 Conclusion

The European Banking Authority and the European Securities and Capital Markets Authority have separately requested rules for cryptocurrency and ICOs to be applied at European level as, in particular, to protect participants in the cryptocurrency system based on blockchain technology.

European authorities recommend to the European Commission that the legal framework applicable to cryptocurrencies to assure a unitary treatment in all European Member States.

It is also recommended that, in case of those cryptocurrencies to which the set of European Union financial rules may apply, European legislation should be adapted to the specific characteristics of cryptocurrencies.

[19] Global legal inside: Blockchain & Cryptocurrency Regulation 2019/Switzerland, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland#chaptercontent2 (last access: 22.7.2019).

## Literature

*Banu, Constantin Mihai/Clem, Filip:* Chamber of Deputies, Department for Parliamentary Studies and EU Policies – EU Division, Study on practical aspects regarding the distributed ledger technology and virtual currencies in the legislation of the European Member States, Bucharest 2019.

*Gibraltar Financial Services Commission:* Distributed Ledger Technology Regulatory Framework, http://www.gfsc.gi/dlt (last access: 22.7. 2019).

*Global legal inside:* Blockchain & Cryptocurrency Regulation 2019/Switzerland, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland#chaptercontent2 (last access: 22.7. 2019).

*Investopedia:* Blockchain, Explained, Investopedia 25.6.2019, https://www.investopedia.com/terms/b/blockchain.asp (last access: 22.7.2019).

*Minister of Communications and Information Society of Romania:* press release on the first institutional meeting between Alexandru Petrescu, the Minister of Communications and Information Society and the representatives of the blockchain industry in Romania, comunicatii.gov.ro 19.3.2019, https://www.comunicatii.gov.ro/prima-intalnire-institutionala-intre-alexandru-petrescu-ministrul-comunicatiilor-si-societatii-informationale-si-reprezentantii-industrie-blockchain-din-romania/ (last access: 22.7.2019).

*National Assembly of France:* Information Report submitted pursuant to art. 145 of the Rules of Procedure by the Joint Information Mission on Blockchains, assemble-nationale.fr 12.12.2018, http://www.assemblee-nationale.fr/15/pdf/rap-info/i1501.pdf (last access: 22.7.2019).

*Walters, Steve:* EU Nations Launch "Mediterranean Seven" In Support Of Blockchain Technology, investinblockchain.com 7.12.2018, https://www.investinblockchain.com/eu-mediterranean-seven/.

# THE DIGITALISATION OF THE ECONOMY AND THE NEEDED REFORM OF THE ECN

Gabriele Carovano*

Organisation for Economic Cooperation and Development (OECD)
Gabriele.Carovano@OECD.org

## Abstract

It is the overriding belief that EU competition rules should be applied uniformly, but reality shows that this is not always the case. Although the European Competition Network (ECN) has functioned successfully during its initial stages, this paper will explore whether it is time to update it, also considering the challenges presented by the 'Digital Revolution'. It seems, indeed, that the so-called 'Digital Revolution' has intensified the risk of non-homogeneous results by raising the number of multinational players, cross-border cases, and new competition issues needing a solution. Simultaneously, this article suggests that enhancing uniformity should not lead to the eradication of diversity. The system should be revamped in a way (i) to valorise diversity as a tool to produce better quality policies and (ii) avoid conflicting decisions. In this sense, the article proposes a possible reform of the ECN to make it able to transform national externalities into European internalities.

## 1 Introduction

Despite the overwhelming view that EU competition law should be uniformly applied, within the EU enforcement system, as represented by the ECN, there is too much room for inconsistency. Notwithstanding the harmonisation of substantial provisions under Article 101, the EU enforcement system remains characterised by (i) different levels of standardisation of substantial rules in respect of Article 102 TFEU, (ii) various national procedural rules both in front of the NCAs and national courts, (iii) the heterogeneity of subjects entrusted to apply competition rules and (iv) the heterogeneity of ways in which the substantial and procedural rules are interpreted and implemented.

Secondly, the risk of inconsistency is increased by the 'digitalisation of the economy' which, with its disruptive effects, is reforming most existing 'brick and mortar markets' as well as introducing new ones as new services

* This article aims to summarise the presentation delivered by its author the 17th May 2019, in Cluj-Napoca, during the 3rd Romanian German Workshop on European Information Law. The presentation was based on the following paper: Carovano Gabriele, The ECN Grand Chamber: Updating the ECN to Face the Challenges of the Online World, European Competition and Regulatory Law 2018, pp. 166-186. The opinions expressed and arguments employed herein are those of the author and do not necessarily reflect the official views of the OECD, the OECD Competition Committee, or the OECD Member countries.

are created. It has also increased the level of integration of national markets by simplifying cross-border purchases of both goods and services and increasing their amount. These changes lead to a situation where every National policy or enforcement decision has a huge impact on other EU Member States' (MSs) consumers and the usual instruments offered by competition law, as they are currently enforced without real coordination, may not be sufficient to ensure a level-playing field and guarantee an effective protection of consumers' decisions.

The above-described inconsistency may compromise the internal market, increase the cost of international trade, raise the threat of externalities and races to the bottom, set back the progress of a unified body of case law and, most importantly, weaken the legal certainty and predictability of EU competition law. Secondly, such inconsistency may generates discrimination among countries and market actors, and mutually delegitimises the decisions of each enforcer.

The inadequateness of the ECN in governing EU heterogeneity has two major causes. Firstly, the network was built with a top-down approach (i.e. it was structured more around the Commission's concerns than around the Network's needs). Secondly, the decisions (if any) taken within it are expressive not of a horizontal, cooperative, consensus-based mechanism but of a hierarchical one.

Several academics criticised the ECN's hierarchical structure[1] and its lack of transparency.[2] Those criticisms are confirmed by the ineptitude of the system both in ensuring consistency in the application of EU competition law across Europe and in solving internal conflicts that may exist within the network. What happened in the *Booking.com case* is a vibrant demonstration of the mentioned phenomena. As stated by some, '*the increased heterogeneity […] inevitably brings an increase in the heterogeneity within the functioning of [the EU's] institutions and policies*'[3] and consequently, it requires a modification of the governance's structure to make it absorbs such a complex and heterogenic integration.

In this scenario, it seems that a more coordinated and convergent European competition enforcement governance, *i.e.* a reformed ECN, is always more necessary and opportune. The 'E-challenges' have proved to be too testing for National answers and solutions should instead come from a

---

1 *Townley*, 33 Yearbook of European Law 1; King's College London Law School Research Paper No. 2014-13; *Cengiz*, ELR 2010, p. 1 (28).

2 *Nazzini*, Competition Enforcement and Procedure, p. 214.

3 *de Búrca/Scott*, in: de Búrca/Scott, Constitutional Change in the Eu: From Uniformity to Flexibility?, p. 1 (2).

complex and reciprocal coordination between Supra-National and National institutions. Hence, an ordered governance of these challenges can only be, to borrow symbology from Kissinger, the result of a balance of local, national or regional partial orders.[4]

Enhancing uniformity, conversely, should not lead to the eradication of diversity. Diversity is a key asset of the European infrastructure, as confirmed by the European motto '*in varietate concordia*', and it must be valued as such. Although the antithesis of one another, uniformity and diversity are both essential. The reformed ECN should encourage the latter and, simultaneously, bridle it to ensure the former. Uniformity, in other words, should be the result of a process refining diversity. Hence, the system should be revamped in a way to make it able of both (i) sponsoring diversity, by encouraging diverse substantive views, also of less experienced NCAs, and (ii) controlling diversity to avoid inconsistency. In this way, the ECN would produce better quality policies and avoid conflicting results. In addition, such a procedure, besides enhancing uniformity, would reduce the public and private cost of multiple-conflicting enforcements while increasing their effects.

Given those premises, this paper will address the issue of whether the current EU competition enforcement system is adequate to ensure consistency and uniformity in the application of EU competition law, especially considering the challenges brought on by the digitalisation of the economy. In answering this question, this article will be divided in three main paragraphs. Paragraph n. 2 describes the main ECN problematics. Paragraph n. 3 explains why the digitalisation of the economy has increased the need of greater co-operation in competition enforcement in Europe. Paragraph n. 4 presents the reform that the author believes to be one of the less distortive solutions to the current ECN's problematics.

## 2 ECN's problematics

### 2.1 ECN's hierarchical structure

The first ECN's issue is its hierarchical structure. The ECN's structure, as noted by Cengiz,[5] is a consequence of the fact that, differently from traditional cooperation networks which naturally emerge, the ECN came into existence as a highly juridical system, designed according to a top-down approach. Indeed, after the decentralization realized by Regulation n. 1/2003, the ECN was created to give the EC a valid instrument through which control how other NCAs would have applied EU competition rules

[4] *Kissinger*, World Order.

[5] *Cengiz*, ELR 2010, p. 1 (2).

and, in case of necessity intervene.[6] This is confirmed by the fact that, differently from traditional multi-level international institutions that produce policies based on agreement and consensus, within the ECN the EC holds a managerial position with powers not shared with the NCAs.[7] Significant from this perspective is Article 11(6), Regulation n. 1/2003, which still preserves one of the central pillar of the old centralized regime by establishing that NCAs must terminate their proceedings if the same case is being investigated by the EC. Similarly, non-infringement decisions (Article 10, Regulation 1/2003) are an exclusive preserve of the EC.

The ECN hierarchical structure, therefore, was a necessary side effect for the establishment of the "decentralized enforcement system", which has some unattended consequences: (i) it may create problematic dominant positions of some members over the others; (ii) it may undermine the network stability; (iii) it may distort the natural interdependencies among actors. The EC intra-network dominant position, as per the so-called "*primus inter pares doctrine*", may make network members, especially the less experienced, unwilling to share their experiences and mistakes.[8] Moreover, the ECN hierarchical structure combined with the absence of an intra-network resolution mechanism lead to other problematics. Indeed, in case of intra-network disagreements, the described situation leads to one of the two options: either the EC directly takes charge of solving the case, thus causing a new centralisation of power going against the spirit of the reformed 'decentralised regime'; or conflicting decisions, express or implied, are inevitable.

The ECN hierarchical structure may also undermine the network stability and the interdependencies among ECN's members.[9] To avoid unequal situations, all ECN members should have identical status and powers, and decisions should be taken based on a consensus-agreement mechanism.

In this scenario, empowering network members to create a 'constitutional level playing field' among themselves is key to making the network run effectively and efficiently. Since at this time a degree of harmony in resources, powers, experiences and independence is still not present within

---

6 *Gabriele*, European Competition and Regulatory Law 2018, pp. 166 (173).

7 *Cengiz*, ELR 2010, p. 1 (3).

8 *Cengiz*, EUI Working Papers, 7; *Gerstenberg/Sabel*, in: Joerges/Dehousse, Good Governance in Europe's Integrated Market, p. 288 (291); *Svetiev*, in: Sabel/Zeitlin, Experimentalist Governance in the European Union: Towards a New Architecture, p. 102 (110).

9 *Gabriele*, European Competition and Regulatory Law 2018, pp. 166 (173).

the ECN,[10] the recent initiative of the EC (so-called ECN Plus Directive[11]) to harmonize and empower NCAs is heartily welcomed. However, this may not be enough. To ensure full network functionality, network members' accountability should be strengthened by compelling them to explain each decision and its impacts on others.

There is also the danger of retaliation and externalities as a result.[12] Transparency and peer review control are essential for discouraging beggar-thy-neighbour strategies.[13] Fox correctly argued that Regulation 1/2003's rules, such as Article 11(6), are there to encourage MSs to consider externalities.[14] The problem with such an approach is that externalities considerations are the result of a hierarchical and heterarchical threat, which has significant consequences on ECN members' spirit of inclusion and perception-conception of those externalities.[15] The hierarchical and heterarchical approach undermines the NCAs' consideration of the ECN as a single body and of being a part of it. In other words, externalities considerations should not be the consequence of a heterarchical and hierarchical threat but the result of an internal self-valuation.

### 2.2 Lack of transparency

The second ECN issue is the lack of transparency with respect to policy and case allocation discussions taking place within network. Starting with the latter, case allocation decisions should be publicly available due to their

[10] *Cengiz*, ELR 2010, p. 1 (3).

[11] European Commission, 'Proposal for a Directive of the European Parliament and of the Council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market' COM(2017) 142 final; Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, OJ L11, 14.1.2019, p. 3-33.

[12] *Townley*, 33 Yearbook of European Law 1; King's College London Law School Research Paper No. 2014-13.

[13] *Scharpf*, in: Joerges/Mény/Weiler, Mountain or Molehill? A Critical Appraisal of the Commission White Paper on Governance, vol Jean Monnet Working Paper No. 6/01 (Robert Schuman Centre for Advanced Studies, EUI 2001), p. 10; See also *Sabel/Zeitlin*, in: Sabel/Zeitlin, Experimentalist Governance in the European Union: Towards a New Architecture, p. 12 (12); *Verdun*, Regulation & Governance 2012, p. 385 (390); *Böge*, in: Ehlermann/Atanasiu, Constructing the EU Network of Competition Authorities, p. 111 (113); *Cengiz*, ECJ, p. 415; *Svetiev*, in: Sabel/Zeitlin, Experimentalist Governance in the European Union: Towards a New Architecture, p. 111 (114).

[14] *Fox*, Legal Issues of Economic Integration, p. 141 (144).

[15] *Rhodes/Visser*, in Héritier/Rhodes, New Modes of Governance in Europe: Governing in the Shadow of Hierarchy, p. 104 (127).

repercussions in terms of right of defence.[16] Jurisdiction in one MS instead of another has consequences on the defendant's side. Here, of course, there is a tension between the need for secrecy, so as not to obstruct ongoing investigations, and the need to publicize the reasoning behind a jurisdiction decision to ensure the right of defence. Although some ECN information, concerning ongoing investigations, is commercially or procedurally sensitive and must not be disclosed, it seems that the current balance of the two interests is all to the advantage of the former. Jurisdiction in one MS instead of another has consequences on the defendant's side. Therefore, it seems appropriate considering a revision of the current balance.

Concerning general policy decisions, to reflect societal concerns and the democratic structure of the legal order, '*deliberation must not take place behind closed doors*'.[17] It is possible that closed groups are needed to build the required mutual trust. By opening them up, there is some risk of endangering this. Transparency, however, will probably 're-politicise' these issues, shifting them from a pure 'technocratic' domain.[18]

### 2.3 Resolution mechanism

The third ECN issue is the absence of an intra-network resolution mechanism to solve internal disagreements whether explicit or implicit. Whereas it is self-evident why explicit conflicting decisions across MSs undermine the uniformity of EU competition law, as in the *Booking.com* case, implicit conflicting decisions deserve deeper analysis.

Implicit conflicting decisions exist when an NCA runs and closes a case adopting an infringement decision not shared in its substance by other ECN actors. They are as damaging as explicit conflicting decisions from a consistency viewpoint. This is the case because, should an NCA decision not be shared by other NCAs, it would engender a conflict between an NCA's decision and other NCA's non-decisions, capable of destabilising the consistency of EU competition law by subjecting the same behaviour acted by the same operator to different treatment among different MSs.

Due to the absence of an intra-network resolution mechanism, the system does not offer any formalised procedure to solve situations where NCAs (i) would struggle to assume jurisdiction, (ii) differ in their substantive analysis, (iii) adopt conflicting decisions, either explicit or implicit.

---

[16] *Nazzini*, Competition Enforcement and Procedure, p. 214.

[17] *Joerges/Neyer*, '"Deliberative Supranationalism" Revisited' EUI Working Paper Law No 2006/20, 4.

[18] *Townley*, 33 Yearbook of European Law 1; King's College London Law School Research Paper No. 2014-13.

Currently, the only available 'safety valve'[19] of the system to prevent or limit the negative effects of intra-network disagreements is Article 11(6), Regulation 1/2003, which states that the EC has the power to advocate cases thus relieving involved NCAs of their jurisdiction in a given case. Article 11(6), however, cannot be considered as a real 'safety valve' since it is expression not of a horizontal, cooperative, consensus-based mechanism but of a hierarchical one. Article 11(6)'s solutions may undermine the trust-based relationships between ECN's members, and cause an advantageous centralisation of power to the EC, contrary to the decentralisation realised by Regulation 1/2003. Unsurprisingly, this power has never been used so far.

## 3 The digitalization of the economy

The digitalisation of the economy increased the necessity of international co-operation for two reasons. Firstly, the majority of firms operating in digital markets are often large businesses operating across borders, which makes co-operation crucial to collect evidence, potentially align remedies, sanctions, and etc. Secondly, competition enforcement against digital firms often involves novel and complex issues (such as algorithm collusion, network effects, two-sided markets, artificial intelligence) which may increase the potential for conflicts between competition enforcers both in terms of methodologies, and outcomes.[20]

Digital markets in the EU have grown steadily over the past years. Between 2000 and 2014, the EU online total retail sales grew at an annual average rate of approximately 22 %.[21] The percentage of individuals making an internet purchase increased from 30 % in 2007, to 55 % in 2016.[22]

---

[19] *Monti*, European Competition Law Annual 2002, p. 3 (8).

[20] *Capobianco/Nyeso*, JECLP 2017, p. 19 (27); *Manyika* et al, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute February 2016), available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows, last access: 20.7.2019 ("Remarkably, digital flows—which were practically nonexistent just 15 years ago—now exert a larger impact on GDP growth than the centuries-old trade in goods"); Digital Competition Expert Panel of the UK, Report "Unlocking digital competition", March 2019, p. 122-123 (recommended action n. 19), available at: https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel.

[21] *Duch-Brown/Martens*, Joint Research Centre of the European Commission, Institute for Prospective Technological Studies, Digital Economy Working Paper 2015/17, JRC 98723.

[22] Eurostat Community Survey on ICT usage in households and by individuals (2016). See also Flash Eurobarometer 397 (2015), Consumers attitude towards cross-border trade and consumer protection.

National markets are not uniform. E-commerce in the EU is geographically concentrated: the United Kingdom, Germany and France account for more than 60 % of EU online sales.[23] The highest percentage of online buyers can be found in the United Kingdom and the lowest in Romania.[24] Data shows that there is a correlation between the percentage of online engaged customers and the internet penetration rate.[25]

In 2016, the number of users buying goods or services for private use over the internet in Europe has increased to 66 %.[26] Of this, 18 %, almost a third, was cross-border.[27] This was reached even though: (i) companies establish barriers to cross-border online trade;[28] (ii) only 37 % of websites allow cross-border purchases;[29] (iii) companies selling cross-border encounter many cost-related difficulties.[30] Cross-border purchases also vary significantly between MSs. While 70 % of residents of Luxembourg engage in cross-border online shopping, only 2 % of Romanian residents do the same. Ordinarily, intensity of cross-border e-commerce is inversely related to population size.[31]

Digital contents in the EU accounted for 32 % of personal online purchases in 2014.[32] A total of 40 % of individuals used the internet to access media content online in 2014, up from 21 % in 2007.[33] Consumer spending

---

[23] *Duch-Brown/Martens*, Joint Research Centre of the European Commission, Institute for Prospective Technological Studies, Digital Economy Working Paper 2015/17, JRC 98723.

[24] Ibid.

[25] Eurostat Community Survey on ICT usage in households and by individuals (2016). See also Flash Eurobarometer 397 (2015), Consumers attitude towards cross-border trade and consumer protection.

[26] Eurostat Community Survey on ICT usage in households and by individuals (2016). See also Flash Eurobarometer 397 (2015), Consumers attitude towards cross-border trade and consumer protection.

[27] Eurostat Community Survey on ICT usage in households and by individuals (2014).

[28] Flash Eurobarometer 413 (2015).

[29] Mystery shopping survey on territorial restrictions and geo-blocking in the European digital single market, (2016); See also *Cardona/Martens*, Joint Research Centre of the European Commission, Institute for Prospective Technological Studies, Digital Economy Working Paper 2014, JRC 92294.

[30] Flash Eurobarometer 413 (2015).

[31] *Duch-Brown/Martens*, Joint Research Centre of the European Commission, Institute for Prospective Technological Studies, Digital Economy Working Paper 2015/17, JRC 98723.

[32] European Commission, Digital Agenda Scoreboard.

[33] Eurostat data on internet usage in the EU-28.

on digital video increased by 400 % between 2010 and 2013.[34] In 2013 alone, spending on digital video subscriptions increased by 147 %.[35] Consumer spending on video subscription services rose by 113 % per year between 2010 and 2014.[36] The number of users grew by 56 % between 2014 and 2015.[37]

Based on this data, some features of these markets can be understood: (i) 'Digital Markets' are growing very fast, transforming markets' business strategies and the society in their entirety; (ii) 'Digital Markets' are not uniformly developed across Europe; (iii) the biggest players of this 'Digital World' are usually huge multinationals which end up forming a new kind of 'natural monopoly' due to the relevance played by network effects and data storage and processing skills;[38] (iii) 'Digital Markets' are highly concentrated, fast-evolving, and require a timely enforcement;[39] (iv) "Digital Markets" present a new range of challenges for competition enforcers; (v) 'Digital Markets' do not respect national borders; (vi) public enforcement in a 'National Digital Market' will also produce effects also in other MSs. This effect is reinforced by Regulation 1/2003 which does not impose territorial limitations to the Commission or NCAs' enforcement powers, *i.e.* they can investigate cases and apply fines for effects beyond their national markets.[40]

Competition Authorities are fully aware of the complex, supra-national dimension of the challenges brought on by the digitalisation of the economy. Unsurprisingly, over the last decade several NCAs have increased their degree of co-operation and mutual assistance. Evidence of this phenomena are: (i) the increased ECN's activities, most of which took place

[34] https://www.google.co.uk/#q=Creating+a+Digital+Single+Market+Bringing+down+barriers+to+unlock+online+opportunities.

[35] See https://www.google.co.uk/#q=Creating+a+Digital+Single+Market+Bringing+down+barriers+to+unlock+online+opportunities.

[36] See http://mouillere.com/universconvergents/wp-content/uploads/2017/03/PortabilityfactsheetDSMpdf.pdf.

[37] See http://mouillere.com/universconvergents/wp-content/uploads/2017/03/PortabilityfactsheetDSMpdf.pdf.

[38] *Naughton*, 22nd May 2017, conference on 'Online Markets and Offline Welfare Effects', University of Oxford Centre for Competition Law and Policy.

[39] *Minton Beddoes*, The Economist, 4th May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last access: 20.7. 2019).

[40] OFT, Guidance as to the appropriate amount of a penalty, OFT423, September 2012, para 2.10.

since 2012 onward;[41] (ii) the first samples of parallel cases;[42] (iii) the first samples of joint sector inquiry on implications of algorithms and big-data on competition;[43] (v) the European Commission's Sector Inquiry on E-commerce, at para 75, acknowledged that *'in the light of the results of the e-commerce sector inquiry, the Commission will broaden the dialogue with national competition authorities within the European competition network on e-commerce-related enforcement to contribute to a consistent application of the EU competition rules as regards e-commerce-related business practices'*.[44]

In conclusion, it appears that the digitalisation of the economy has increased the need for co-operation to ensure consistency and to develop better solutions. 'Digital Markets' vary across MSs, but this does not necessarily justify the adoption of different enforcement regimes by NCAs. Of course, different solutions across different MSs maybe justified given National markets' differentiations. Different solutions, however, are only justified to the extent that material reasons require so. Different solutions, therefore, are transitory in nature and should be treated as exception. In the long term, differently, uniform solutions are needed for the creation of

[41] See: http://ec.europa.eu/competition/ecn/documents.html (last access: 20.7.2019).

[42] Booking.com case: (i) AGCM (2015), Provvedimento n. 25940; (ii) Autorité de la Concurrence (2015), Decision available at: http://www.autoritedelaconcurrence.fr/pdf/avis/15d06.pdf; (iii) Konkurrensverket (2015), English Decision available at: http://www.konkurrensverket.se/globalassets/english/news/13_596_bookingdotcom_eng.pdf (last access: 20.7.2019).; (iv) Bundeskartellamt (2015), Press release of 23 December 2015 and English Decision available at: http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Kartellverbot/B9-66-10.pdf%3F__blob%3DpublicationFile%26v%3D3 (last access: 20.7.2019); the Amazon case: http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2013/26_11_2013_Amazon-Verfahrenseinstellung.html%3Fnn%3D3599398 (last access: 20.7.2019) and https://www.gov.uk/cma-cases/amazon-online-retailer-investigation-into-anti-competitive-practices (last access: 20.7.2019); the Adidas case: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2014/02_07_2014_adidas.html (last access: 20.7.2019). and http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Kartellverbot/2014/B3-137-12.pdf?__blob=publicationFile&v=2 (last access: 20.7.2019). and http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=607&id_article=2671; the Online Ticket ing case:http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen /2016/22_03_2016_DFB.ht ml?nn=3599398 (last access: 20.7.2019).and http://www.bu ndeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2014/30_01_2014_Fah rkartenvertrieb_DB.html (last access: 20.7.2019).and https://www.ccpc.ie/business/ccpc-commences-formal-investigation-suspected-anti-competitive-conduct-ticketing-sector/ (last access: 20.7.2019).

[43] See http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf; http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/10_05_2016_Big%20Data%20Papier.html (last access: 20.7.2019); https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/19_06_2018_Algorithmen.html (last access: 20.7.2019).

[44] European Commission, 'Sector Inquiry on E-commerce' COM(2017) 229 final.

a level playing field across MSs and, ultimately, of a 'Single Digital Market'. Secondly, admitting that different solutions can exist does not mean that the competition enforcement system should be devoid of any mechanism to prevent them where they are not strictly necessary.

## 4 The ECN Grand Chamber

Having described the ECN's problematics, and understood how they have been intensified by the digitalisation of the economy, it is now time to start considering which potential solution maybe adopted to solve the mentioned problematics. The ECN needs to be restructured in a way to be able to (i) equalise the position of every ECN's member within the network by abolishing its hierarchical structure (ii) sponsor diversity to ensure experimentation and innovation of solutions;[45] (iii) drive and control diversity to guarantee consistency and legal certainty; (iv) reduce the costs of public enforcement both for private companies and for NCAs; (v) increase deterrence, effectiveness, and efficiencies of EU competition public enforcement; (vi) increase the positive synergies of the interaction between public and private enforcement. The solution identified by the author of this paper as the best compromised between the need to innovate and that of preserving the positive aspects of the current enforcement system is the introduction of the 'ECN Grand Chamber'.

The 'ECN Grand Chamber' would work as a 'resolution mechanism' capable of replacing Art. 11(6), and of pushing forward the current 'Advisory Committee' *ex* Art. 14, Regulation 1/2003. Its structure should be similar to that of the ECJ when called upon to decide a matter of law in its Grand Chamber conformation. The 'ECN Grand Chamber' should be made up of a President, one or more Vice-Presidents, and, a minimum of one representative for each ECN member with full authority to act on behalf of its NCA. The President and Vice-Presidents should be chosen randomly, respecting a rotation order to guarantee each NCA representative has an equal chance of being selected. The President and Vice-Presidents must control, coordinate, and lead the ECN Grand Chamber's activities, in particular ensuring that each NCA and the EC have the same rights and duties within the Grand Chamber. Moreover, it is up to the President to decide whether, when, and how the ECN Grand Chamber hearings should be public and/or the related discussions publicised.

The EC should oversee referrals to the Grand Chamber, which could be convened (at least) for three different purposes:

[45] *Sabel/Zeitlin*, in: Sabel/Zeitlin, Experimentalist Governance in the European Union: Towards a New Architecture, p. 1 (9 f.).

(1) either to solve a jurisdiction issue in case of disagreement during case allocation discussions, or to solve a conflict between NCAs or between the EC and NCAs and vice versa, regarding: (i) how new competition issues should be addressed; (ii) whether competition law should be applied in a particular sector; (iii) whether an investigation should be stopped or carried out in a different way. The ECN Grand Chamber, therefore, could be called on for every kind of dispute within the ECN (Type 1 scenario). In this first scenario, the ECN Grand Chamber may be convened upon request of the EC or at least five NCAs. This convocation mechanism is deliberately devised to avoid an overuse of this procedure and should be used with caution and parsimony.[46] It should be considered as an 'extrema ratio' procedure.

(2) To expand the territorial effects of an NCA's decision across Europe (Type 2 scenario), in which case the ECN Grand Chamber could be convened upon request of the sole acting NCA. An acting NCA could convene the ECN Grand Chamber to have its line of enforcement and conclusions shared by its colleagues. Should the 'a quo' NCA be successful, its decision would produce effects across Europe and be binding for all National Courts of each MSs within the meaning of Art. 9(1), Damages Directive.[47] However, were the 'a quo' NCA not successful, it would have to undergo and comply with the solution adopted by the ECN Grand Chamber.

(3) At the beginning of each enforcement year to define EU enforcement priorities (Type 3 scenario).

To make sure that the current hierarchical ECN structure is abolished, and to favour participation of each NCA, even the less experienced, the ECN Grand Chamber's decisions should be taken according to a voting system very similar to the one adopted by the European Council on 1st November 2014. According to this procedure for Qualified Majority Voting, a proposal would be approved if 55 % of ECN members vote in favour. Each competition authority's vote would have the same value to ensure equality. The solution or the position of the Authority presenting the strongest argument and most agreed on by the ECN's members would be the one adopted.

In exceptional cases, where not all ECN members participate in the vote, a decision would be approved if 55 % of the participating ECN members

[46] In this sense, for the US, *Kovacic*, Competition Law International 2008, p. 8 (10).

[47] Under the current regime, according to Art. 9(2), Damages Directive, a final decision of an NCA does not have a binding effect before National Courts of another Member State but it is downgraded to a prima facie evidence that an infringement of competition law has occurred. Therefore, extending the binding effect of decisions of NCAs outside the national jurisdiction of the authority which has taken the decision will boost private enforcement actions.

voted in favour. An abstention under qualified majority voting would count as a vote against. Abstention is not the same as not participating in the vote.[48] Any ECN member could abstain at any time. The existence of a blocking minority should also be considered. It would exist when the EC, plus more than 40 % of the ECN members, ie 12 NCAs at least, voted against the proposal. Whether a QM was not reached after the first round or if it was, but a blocking minority existed, the ECN members would be called to a second-round voting. In the second-round voting, the EC would enjoy an extraordinary vote power, and the proposal will be approved by a simple majority of 51 %. Notably, the EC vote would count for as many as three votes of an NCA. This mechanism will ensure that: (i) stall situations will be overcome; (ii) the EC will drive uncertain situations; (iii) the EC will preserve its role as 'Guardian of the Treaties'.

There also are other situations where the ECN Grand Chamber could provide additional benefits. Firstly, it could be used, for instance, by NCAs to force the EC to review some of its positions, a power not offered by the current framework as designed by Regulation 1/2003. This possibility would increase the debate, therefore, diversity, also for situations where under the current system no experimentation at all is allowed to NCAs when the EC handles a case. Thus, the proposed reform: (i) would boost diversity and experimentation; (ii) would eliminate the hierarchical structure of the current system by equalising the NCAs with the EC, without undermining its role as 'Guardian of the Treaties'. This Guardian position, indeed, would be ensured by the fact that: (i) the EC would oversee the applications for convening the ECN Grand Chamber; (ii) the EC could convene the ECN Grand Chamber by itself; (iii) the EC would have special vote power during the second-round voting.

Secondly, the Grand Chamber could be used by the EC to stop action by an NCA believed to be premature, unnecessary or wrong. Also, this power is not available under the current regime *ex* Regulation 1/2003. Under Art. 11(6) the Commission can advocate a case, so relieving the acting NCA of its power, but the EC cannot stop it exclusively. This may be an additional tool at the EC's or other NCAs' disposal to slow down enforcement activities when the understanding of the competition issues or solutions behind that case is still not clear.

In conclusion, it seems to the author of this paper that the proposed reform is a good compromise between the need to preserve the positive aspects of the current system and that to realise the sorely-needed upgrade of the ECN. The ECN Grand Chamber mechanism, while preserving all the

[48] The difference is that being present influences the quorum of 55 % while being absent can reduce that quorum.

benefits of the current system as designed by Regulation 1/2003, also seems able to fulfil all the objectives mentioned at the beginning of this section.

## Literature

*Böge, Ulf:* The Bundeskartellamt and the Competition Authorities of the German Länder, in: Claus Dieter Ehlermann/Isabela Atanasiu (eds), Constructing the EU Network of Competition Authorities, Hart 2002, pp. 111-118.

*Capobianco, Antonio/Nyeso, Anita:* Challenges for Competition Law Enforcement and Policy in the Digital Economy, JECLP 2017, pp. 19-27.

*Cengiz, First:* Multi-level governance in competition policy: the European Competition Network, European Law Review 2010, pp. 660-677.

*Cengiz, First:* The European Competition Network: Structure, Management and Initial Experiences of Policy Enforcement, EUI Working Papers 2009.

*de Búrca, Gráinne/Scott, Joanne:* Introduction, in: Gráinne de Búrca,/Joanne Scott (eds), Constitutional Change in the Eu: From Uniformity to Flexibility?, Hart 2000, pp. 1-9.

*Digital Competition Expert Panel of the UK:* Report"Unlocking digital competition", March 2019.

*Duch-Brown, Nestor/Martens, Bertin*: The European Digital Single Market: its Role in Economic Activity in the EU, Joint Research Centre of the European Commission, Institute for Prospective Technological Studies, Digital Economy Working Paper 2015/17, JRC 98723.

*Fox, Eleanor:* The Elusive Promise of Modernisation: Europe and the World, Legal Issues of Economic Integration 2001, pp. 141-149.

*Gabriele, Carovano:* The ECN Grand Chamber: Updating the ECN to Face the Challenges of the Online World, European Competition and Regulatory Law, Volume 2, Issue 3 (2018), pp. 166-186.

*Gerstenberg, Oliver/Sabel, Charles:* Directly-Deliberative Polyarchy: An Institutional Ideal for Europe?, in: Christian Joerges/Renaud Dehousse (eds), Good Governance in Europe's Integrated Market, Oxford 2002, pp. 288–341.

*Kissinger, Henry:* World Order, London 2015.

*Kovacic, William:* Competition Policy in the European Union and the United States: Convergence or Divergence in the Future Treatment of Dominant Firms? Competition Law International 2008, pp. 8-18.

*Joerges, Christian/Neyer, Jürgen:* Deliberative Supranationalism, Revisited' EUI Working Paper Law No 2006/20, 4.

*Manyika, James/Lund, Susan/Bughin, Jacques/Woetzel, Jonathan/Stamenov, Kalin /Dhingra, Dhruv*: Digital Globalization: The New Era of Global Flows (McKinsey Global Institute March 2016) available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows (last access: 20.7.2019).

*Minton Beddoes, Zanny:* 'The world's most valuable resources: data and the new rules of competition', The Economist, 4th May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last access: 20.7.2019).

*Monti, Mario:* 'The Network Concept, Competition Authority Networks and Other Regulatory Networks', European Competition Law Annual 2002, pp. 3-10.

*Nazzini, Renato:* Competition Enforcement and Procedure, Oxford 2016.

*Rhodes, Martin/Visser, Jelle*: Seeking Commitment, Effectiveness and Legitimacy: New Modes of Socio-Economic Governance in Europe, in: Adrienne Héritier/Martin Rhodes (eds), New Modes of Governance in Europe: Governing in the Shadow of Hierarchy, Basingstoke 2011, pp. 104-134.

*Sabel, Charles F./Zeitlin Jonathan:* Learning from Difference: The New Architecture of Experimentalist Governance in the Eu, in: Charles F. Sabel/ Jonathan Zeitlin (eds), Experimentalist Governance in the European Union: Towards a New Architecture, Oxford 2010, pp. 1-28.

*Scharpf, Fritz:* European Governance: Common Concerns Vs. The Challenge of Diversity, in: Christian Joerges/Yves Mény/Joseph Weiler (eds), Mountain or Molehill? A Critical Appraisal of the Commission White Paper on Governance, vol Jean Monnet Working Paper No. 6/01 (Robert Schuman Centre for Advanced Studies, EUI 2001).

*Svetiev, Yane:* Networked Competition Governance in the Eu: Delegation, Decentralisation, or Experimentalist Architecture?, in: Charles Sabel/ Jonathan Zeitlin (eds), Experimentalist Governance in the European Union: Towards a New Architecture, Oxford 2010, p. 79-120.

*Townley, Christopher:* Co-ordinated Diversity: Revolutionary Suggestions for EU Competition Law (and for EU Law too), 33 Yearbook of European Law 1; King's College London Law School Research Paper No. 2014-13.

*Verdun, Amy:* Experimentalist Governance in the European Union: A Commentary, Regulation & Governance 2012, pp. 385–393.