Monitoring VoIP

Internet-Telefonie unter Beobachtung

Wolfgang Däubler

Internet-Telefonie gewinnt immer mehr an Bedeutung. Das hängt mit den geringen Kosten zusammen. Allerdings gibt es auch Störungen, denen der Arbeitgeber auf den Grund gehen will. Wie er dies nicht tun darf, soll im Folgenden dargestellt werden.

Der Ausgangspunkt: VoIP in der Pilotphase

In der Zentrale des Konzerns X und in vier Tochtergesellschaften wird seit 2012 probeweise Internet-Telefonie praktiziert. Wenn die Sache im Ergebnis glatt läuft, sollen alle Konzernunternehmen einbezogen werden.

In der Praxis hat sich herausgestellt, dass das neue System für Störungen recht anfällig ist. Anders als beim klassischen Telefonieren wird kein eigenes Medium zur Übertragung von Sprache genutzt.[1] Die Konzernleitung beabsichtigt daher, eine sog. Quality Monitoring Software einzusetzen. Sie soll die Verbindungsqualität von VoIP-Gesprächen erfassen und bei Störungen rechtzeitige Gegenmaßnahmen möglich machen. Da auch Arbeitnehmerdaten betroffen sind, wurde der KBR um Zustimmung gebeten. In ihrem Schreiben umreißt sie das Funktionieren der Software wie folgt:

„Die Qualität von VoIP-Gesprächen nimmt drastisch ab, wenn Sprachpakete nicht zeitnah empfangen werden, wenn Pakete verloren gehen oder in falscher Reihenfolge empfangen werden. Eine VoIP Quality Monitoring Software hilft, schnell auf mögliche Probleme zu reagieren und so eine hohe Gesprächsqualität sicherzustellen... Nur durch ständige Beobachtung und automatische Alarmierung bei Verschlechterungen ist eine proaktive Reaktion möglich, also noch bevor es Beschwerden durch die Nutzer des Systems gibt.
Dazu senden die einzelnen VoIP-Telefone am Ende des Gesprächs eine Protokolldatei an einen hierfür bereitgestellten Server.
Diese Protokolldatei wird folgende Daten enthalten:
- Die Rufnummern bzw. IP-Adressen der beiden Gesprächspartner
- Datum und Uhrzeit des Anrufs
- Dauer des Anrufs.
Inhalte von Telefongesprächen sollen nicht gespeichert werden.“

Zur rechtlichen Begründung wurde auf § 100 TKG verwiesen. Nach dieser Bestimmung darf der Anbieter von Telekommunikationsdienstleistungen zum „Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.“ Die auf diese Weise erfassten Daten dürften nicht für andere Zwecke verwendet werden.

[1] Gute Einführung auch in die technische Seite bei Barroso de Souza/Greve/Schertel/Wedde, Voice overIP. Handlungsmöglichkeiten des Betriebs-/Personalrats bei Internettelefonie, Düsseldorf 2014 (verdi b+b)

Die Daten sollten - so heißt es weiter in dem Schreiben - für die Dauer von sechs Monaten gespeichert und anschließend gelöscht werden. Auf diese Weise solle eine schleichende Verschlechterung z. B. durch allmähliche Überlastung von Leitungen erkennbar werden. Sobald die Qualität der Telefongespräche einen bestimmten Schwellenwert unterschreite, würde eine Warnmeldung erfolgen, die ausschließlich an die VoIP-Administratoren gehe.

Mitbestimmungsrecht des Betriebsrats

Beide Seiten waren sich darüber einig, dass die Einführung der Quality Monitoring Software mitbestimmungspflichtig ist. Dies folgt aus § 87 Abs. 1 Nr. 6 BetrVG, der es bereits genügen lässt, dass eine technische Einrichtung geeignet ist, Verhalten und Leistung der Arbeitnehmer zu überwachen; auf die Absichten des Arbeitgebers kommt es nicht an.[2] Das Mitbestimmungsrecht greift auch dann ein, wenn ein bereits bestehendes System erweitert und zusätzliche Daten gespeichert oder zusätzliche Verwertungsmöglichkeiten eröffnet werden.[3] Genau dies ist bei der Quality Monitoring Software der Fall.

Unstreitig war weiter die Zuständigkeit des Konzernbetriebsrats nach § 58 Abs. 1 BetrVG, da sich die in Rede stehende Maßnahme nicht nur auf ein Unternehmen erstreckte; gleichzeitig war eine einheitliche Lösung für die „Stabilisierung“ und Störungsfreiheit des Systems zwingend geboten. Für den KBR stellte sich als erstes die Frage, ob die beabsichtigte Datenspeicherung überhaupt zulässig ist. Sein Mitbestimmungsrecht hat gerade auch den Sinn, Verletzungen des Datenschutzes zu verhindern.

Die erfassten Daten

Die beabsichtigte Speicherung der Rufnummern bzw. der IP-Adressen beider Gesprächspartner betrifft Daten, die nicht unmittelbar auf bestimmte Arbeitnehmer verweisen, die jedoch unter Heranziehung von Listen und anderem „Zusatzwissen“ unschwer auf

---

[2] So seit BAG v. 9.9.1975 – 1 ABR 20/74 – AP Nr. 2 zu § 87 BetrVG 1972 Überwachung, das BAG in ständiger Rechtsprechung; zuletzt BAG v. 10.12.2013 – 1 ABR 43/12 – NZA 2014, 439 Tz. 20

[3] LAG Düsseldorf v. 14.12.1981 – 26 TaBV 80/81 – EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 10 (S. 73). Für das BAG (v. 14.9.1984 – 1 ABR 23/82 – AP Nr. 9 zu § 87 BetrVG 1972 Überwachung) war die Mitbestimmungspflichtigkeit dieses Tatbestands so selbstverständlich, dass es in einem einschlägigen Fall darüber kein Wort verlor.

bestimmte Beschäftigte bezogen werden können. Insoweit besteht rechtlich kein Unterschied. § 3 Abs. 1 BDSG lässt es genügen, wenn Einzelangaben über persönliche oder sachliche Verhältnisse einer „bestimmbaren" natürlichen Person zugeordnet werden können. Auch (dynamische) IP-Adressen werden von der Rechtsprechung des BGH als personenbeziehbare Daten behandelt.[4] Genauso sind „Datum und Uhrzeit des Anrufs" sowie die Dauer des Gesprächs zu behandeln, die ja gleichfalls gespeichert werden sollen.

Werden personenbezogene Daten erfasst, so greift im Normalfall das BDSG ein. Geht es um Telekommunikation, so stellt sich allerdings die Frage, ob nicht die Spezialnormen der §§ 88 ff. TKG eingreifen. Dies ist in der Tat der Fall, soweit im Betrieb Privatgespräche erlaubt oder zumindest geduldet werden: Hier ist der Arbeitgeber Anbieter von Telekommunikationsleistungen. Bei Dienstgesprächen gilt dies nicht; hier findet nur der allgemeine Persönlichkeitsschutz Anwendung, wie er im informationellen Selbstbestimmungsrecht und im BDSG zum Ausdruck gekommen ist.[5] Da sich die Arbeitgeberseite auf § 100 TKG beruft, geht sie selbst davon aus, dass Privatgespräche zulässig sind. Ob bei ihnen eine sechsmonatige Speicherung der „Verkehrsdaten" zulässig ist, soll als erstes untersucht werden.

Erfassung der Daten von Privatgesprächen

Privatgespräche unterfallen dem Schutz des Telekommunikationsgeheimnisses nach § 88 TKG, das den Art. 10 GG konkretisiert. Eingriffe müssen einen legitimen Zweck verfolgen und dem Verhältnismäßigkeitsprinzip Rechnung tragen. Im konkreten Fall geht es um die Störungsprävention und die Störungsbeseitigung im Sinne des § 100 Abs. 1 TKG; gegen diesen Zweck ist nichts einzuwenden. Das eigentliche Problem liegt im Verhältnismäßigkeitsprinzip, das – wie die Eingangsworte „soweit erforderlich" dokumentieren – auch im Rahmen des § 100 TKG zu beachten ist.[6] Im Einzelfall kann es angesichts komplexer technischer Vorgänge zweifelhaft sein, ob eine bestimmte Maßnahme zur Erreichung des Zwecks geeignet und erforderlich ist. In diesem Fall ist es Sache des Arbeitgebers, dies im Einzelnen darzulegen und zu beweisen; ggf. muss er einen Sachverständigen heranziehen. Dies folgt schon aus dem Ausnahmecharakter des § 100

[4] BGH v. 13. 1. 2011 – III ZR 146/10 – NJW 2011, 1509 ff.
[5] Näher dazu Däubler CuA 11/2014 S. 4 ff.
[6] BGH v. 13. 1. 2011 – III ZR 146/10 – NJW 2011, 1509, 1512 Tz. 27; zustimmend Jenny, in: Plath (Hrsg.), BDSG-Kommentar, Köln 2013, § 100 TKG Rn. 6

Abs. 1 TKG, der von der Regel des § 96 Abs. 1 Satz 3 TKG abweicht, wonach Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen sind.[7]

Unterstellen wir, die Software sei für den beabsichtigten Zweck geeignet, so fehlt es gleichwohl an der Erforderlichkeit. Weshalb müssen die Telefondaten „flächendeckend" gespeichert, also grundsätzlich alle Nebenstellen und alle Uhrzeiten erfasst werden? Wäre es nicht ein weniger belastendes Mittel, einen bestimmten Grenzwert für die Übertragungsqualität zu wählen, bei dessen Unterschreitung die Aufzeichnungen beginnen? Sobald durch eine weitere Verschlechterung der heute maßgebende Grenzwert erreicht wäre, könnte die Auswertung beginnen – ihre Geeignetheit als Grundlage für sachgerechte Maßnahmen immer unterstellt.

Offen ist weiter, welche Maßnahmen in Betracht kommen, um die Überlastung und die dadurch bedingte geringere Übertragungsqualität zu bekämpfen. Werden einzelne Anschlussinhaber aufgefordert, weniger als bisher zu telefonieren oder auf andere Geräte zurückzugreifen? Wäre dies der Fall, läge der Überwachungscharakter offen zutage. Gibt es andere Wege, die einen solchen „Durchgriff" auf den Einzelnen vermeiden? Wie wären diese beschaffen? Dazu hat die Arbeitgeberseite bisher nichts ausgeführt.

Von diesen Bedenken ganz abgesehen, ist auch die Verhältnismäßigkeit im engeren Sinne nicht gewahrt. Bei ihr kommt es darauf an, ob die verfolgten Ziele in einem angemessenen Verhältnis zur Tragweite des Grundrechtseingriffs stehen, der dem Einzelnen zugemutet wird. Im vorliegenden Fall geht es ausschließlich um das bessere Funktionieren der Telefonanlage. In anderen von der Rechtsprechung entschiedenen Fällen standen höher zu gewichtende Interessen auf dem Spiel, die jedoch nicht in der Lage waren, vergleichbar weitreichende Eingriffe zu rechtfertigen.

In dem vom BGH entschiedenen Fall ging es insbesondere um die Abwehr von Schadprogrammen, Spam-Mails und „Denial-of-Service-Attacken".[8] In der Entscheidung des BVerfG zur Vorratsdatenspeicherung handelte es sich weitergehend um die Ermittlung und Abwehr schwerster Straftaten und damit um überragend wichtige Aufgaben des Rechtsgüterschutzes.[9]

[7] So ausdrücklich auch für den Fall des § 100 TKG BGH v. 13. 1. 2011 – III ZR 146/10 - NJW 2011, 1509, 1511 Tz. 19 in Verbindung mit Tz. 12 m. w. N.
[8] S. Fußnote 7 Tz. 24
[9] BVerfG v. 2. 3. 2010 – 1 BvR 256/08 – NJW 2010, 833 ff.

Auf der anderen Seite war der Eingriff im Falle des BGH von sehr viel geringerem Gewicht. Das Gericht hatte nur über die Erfassung von IP-Adressen zu entscheiden, während im vorliegenden Fall die Nummern bzw. Adressen des Anrufers wie des Angerufenen, Beginn und Ende des Gesprächs sowie seine Dauer erfasst werden. Dies lässt sehr viel genauere Rückschlüsse über das Verhalten des Betroffenen zu als die bloße Speicherung der IP-Adressen. Dazu kommt der Zeitraum der Speicherung. Während es in dem vom BGH entschiedenen Fall darum ging, dass die Daten für eine Woche gespeichert und anschließend automatisch gelöscht wurden, geht es hier um eine Speicherung für die Dauer von sechs Monaten. Dies entspricht exakt der Frist, die zunächst für die Vorratsdatenspeicherung vorgesehen war. Sie sollte der Ermittlung schwerster Straftaten dienen, wurde aber vom Bundesverfassungsgericht wegen Verstoßes gegen das Verhältnismäßigkeitsprinzip als grundrechtswidrig qualifiziert und aufgehoben. Was nicht einmal für Zwecke der Terrorismusbekämpfung zulässig ist, kann beim besten Willen nicht akzeptiert werden, wenn es nur um die Optimierung einer Telefonanlage geht. Nach den Maßstäben des Bundesverfassungsgerichts liegt die Unverhältnismäßigkeit auf der Hand.

Erfassung der Daten von Dienstgesprächen

Soweit Telefongespräche zu dienstlichen Zwecken geführt werden, greift das TKG nicht ein. Die Konzernleitung kann sich daher nicht auf dessen § 100 berufen. Auch das Grundrecht aus Art. 10 Abs. 1 GG (Fernsprechgeheimnis) ist nicht einschlägig, da der Arbeitnehmer nicht Inhaber des fraglichen Anschlusses ist. Insoweit gilt nur der allgemeine Persönlichkeitsschutz, der auch die Vertraulichkeit von Telefongesprächen erfasst. Nach der Rechtsprechung des Bundesverfassungsgerichts[10] kann sich ein Arbeitnehmer auch dann auf sein „Recht am eigenen Wort“ berufen, wenn er Dienstgespräche führt. Soweit die Begleitumstände seiner Telefongespräche gespeichert und verarbeitet werden, ist sein informationelles Selbstbestimmungsrecht betroffen.

Als Rechtsgrundlage für die Erhebung und Verarbeitung der Daten von Beschäftigten kommt allein § 32 Abs. 1 Satz 1 BDSG in Betracht. Auch diese Vorschrift ermöglicht die Erfassung und Verarbeitung von Arbeitnehmerdaten nur unter dem Vorbehalt des „Erforderlichen“. Dies

---

[10] BVerfG v. 19. 12. 1991 – 1 BvR 382/85 – DB 1992, 786 = CR 1992, 498 ff., bestätigt durch BVerfG v. 9. 10. 2002 – 1 BvR 1611/96 und 1 BvR 805/98 – NJW 2002, 3619 = DuD 2003, 170

ist nicht anders als im Rahmen des § 100 Abs. 1 TKG zu verstehen: Die vorgesehenen Maßnahmen müssen geeignet, erforderlich und verhältnismäßig im engeren Sinne sein.[11] Die Bedenken, die oben im Rahmen des § 100 Abs. 1 TKG deutlich wurden, gelten hier in gleicher Weise. Auch im Arbeitsverhältnis muss der Arbeitgeber beweisen, dass die Voraussetzungen für einen Eingriff in Arbeitnehmerrechte (hier: in das informationelle Selbstbestimmungsrecht) gegeben sind. Auch hier gilt der Grundsatz des mildesten Mittels, wonach die Zahl der erfassten Daten ebenso wie der Umfang der Auswertung möglichst gering zu halten sind. Auch hier darf die Tragweite des Eingriffs nicht außer Verhältnis zu dem verfolgten Zweck stehen.

Überprüfung am Maßstab des Unionsrechts?

Art. 7 der EU-Grundrechte-Charta gibt jeder Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Werden Daten der hier interessierenden Art erhoben und gespeichert, so wird nach der Rechtsprechung des EuGH in dieses Grundrecht eingegriffen; das ist im Zusammenhang mit der durch die Richtlinie 2006/24 vorgeschriebenen Vorratsdatenspeicherung ausdrücklich festgestellt worden.[12] Betroffen ist weiter das Grundrecht auf Datenschutz nach Art. 8 Abs. 1 der EU-Grundrechte-Charta, das neben Art. 7 der Charta Anwendung findet.[13]

Fraglich könnte sein, ob diese unionsrechtlichen Grundrechte im vorliegenden Fall eingreifen. Nach Art. 51 Abs. 1 der Grundrechte-Charta sind die Mitgliedstaaten an die Charta nur gebunden, soweit sie Unionsrecht ausführen. Geht es um Richtlinien, ist dies nicht nur beim Erlass eines Umsetzungsgesetzes, sondern auch dann der Fall, wenn es um die Auslegung des auf der Richtlinie beruhenden Rechts geht, das insoweit nicht in Widerspruch zum Unionsrecht geraten darf.[14]

Das geltende Datenschutzrecht besitzt in Form der „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der

---

[11] Forst, in: Auernhammer (Begr.), BDSG, Kommentar, Köln u. a. 2014, § 32 Rn. 52 ff. Seifert, in: Simitis (Hrsg.), BDSG, 8. Aufl, Baden-Baden 2014, § 32 Rn. 9 ff.; Zöll, in: Taeger/Gabel (Hrsg.), BDSG und Datenschutzvorschriften des TKG und des TMG, 2. Aufl., Frankfurt/Main 2013, § 32 Rn. 18

[12] EuGH v. 8. 4. 2014 – C-594/12 – NJW 2014, 2169, 2170 Tz. 29

[13] EuGH v. 8. 4. 2014 – C-594/12 – NJW 2014, 2169, 2170 Tz. 29

[14] S. Borowsky, in: Jürgen Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union. Kommentar, 3. Aufl., Baden-Baden 2011, Art. 51 Rn. 27

Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ [15] eine unionsrechtliche Grundlage. Dasselbe gilt für die elektronische Kommunikation; insoweit ist die „Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ einschlägig.[16] Soweit es um die Auslegung datenschutzrechtlicher Normen des BDSG, aber auch spezieller Materien wie des TKG geht, müssen daher Art. 7 und Art. 8 der Grundrechte-Charta beachtet werden.

Maßstäbe für Eingriffe in diese Grundrechte hat der EuGH in seiner Entscheidung zur Vorratsdatenspeicherung entwickelt und in umfassender Weise konkretisiert.[17] Im Grundsatz sind die Eingriffsvoraussetzungen keine anderen als im deutschen Recht, doch werden einige zusätzliche Gesichtspunkte herausgearbeitet, die in unserer Diskussion eine geringere Rolle gespielt haben.

Auch im Unionsrecht geht es neben der Geeignetheit und der Erforderlichkeit um eine Abwägung zwischen den mit einer Maßnahme verfolgten Zielen und der Schwere des Eingriffs in Grundrechte. Beanstandet wurde deshalb, dass alle Verkehrsdaten gleich behandelt wurden und keine Ausnahme (oder mildere Regelung) für Berufsgeheimnisse vorgesehen war, obwohl dort ein tieferer Eingriff vorliegt.[18] Eine solche Differenzierung fehlt auch in dem hier dargestellten Fall. Träger von Berufsgeheimnissen wie z. B. Werksärzte gibt es auch in dem fraglichen Konzern.

Weiter beanstandete der EuGH, es sei unklar, welche Straftaten hinreichend schwer seien, um die von der Richtlinie verlangte Speicherung der Verkehrsdaten auszulösen, und wann eine Zugriffsberechtigung bestehe.[19] Dem würde hier der bisher nicht konkretisierte Grenzwert entsprechen, der zu einem Zugriff auf die gespeicherten Daten berechtigt.

Der EuGH verlangt weiter, dass Personen, deren Daten auf Vorrat gespeichert werden, über ausreichende Garantien verfügen müssen, die einen wirksamen Schutz vor

[15] ABl. Nr. L 281/31
[16] ABl. Nr. L 201/37
[17] EuGH v. 8. 4. 2014 – C-293/12, C-594/12 – NJW 2014, 2169. Zu dieser Entscheidung s. Simitis NJW 2014, 2158 ff.
[18] EuGH, a. a O., Tz. 56 – 58
[19] EuGH, a. a. O., Tz 60, 61

Missbrauchsrisiken sowie vor unberechtigtem Zugang und unberechtigter Nutzung beinhalten.[20] Was den Zugang betrifft, so ist dem Rechnung getragen, da ein eigenständiger Server mit passwortgeschützter Datenbank errichtet wird, auf den nur konkrete VoIP-Administratoren Zugriff haben. Der Schutz vor Missbräuchen ist demgegenüber nicht durch besondere Vorkehrungen sichergestellt, da lediglich bestimmt ist, dass die Daten ausschließlich zur Fehlerbehebung und zu keinerlei anderen Zwecken herangezogen werden dürfen. Wie wird sicher gestellt, dass dieser Grundsatz auch wirklich eingehalten wird?

Im Ergebnis sind sich deutsches und Unionsrecht aber einig: Telefondaten ein halbes Jahr zu speichern, ist ersichtlich unverhältnismäßig.

[20] EuGH, a. a. O., Tz. 54