Markus Kompa
Rechtsanwalt
Fachanwalt für Urheber- und Medienrecht

Geißelstr. 11
50823 Köln
Tel: 49-221-29960001
Fax: 49-221-29960002
info@kanzleikompa.de

Bankverbindung:
Sparkasse KölnBonn
DE41 3705 0198 0815 0008 36
COLSDE33XXX
StIdNr: 56 263 087 916

RA Markus Kompa • Geißelstr. 11 • 50823 Köln

An die

Staatsanwaltschaft Bonn

53222 Bonn vorab per Fax: 0228-9752-600

Ihre Zeichen, Ihre Nachricht vom	Unser Zeichen, unsere Nachricht vom	Telefon, Name	Datum
	DC 2/17	(0221) 29960001, Kompa	16.06.2017

Straf- und Ordnungswidrigkeitsanzeige wegen Verstoßes gegen § 6b BDSG

Sehr geehrte Damen und Herren,

unter Vorlage anliegender Vollmachtsurkunde zeige ich Ihnen die anwaltliche Vertretung des Digitalcourage e.V., vertreten durch den Vorstand, Marktstraße 18, 33602 Bielefeld, an,

und erstatte für meine Mandantschaft hiermit

Strafanzeige bzw. Ordnungswidrigkeitenanzeige

gegen

1. Herrn Dr. Frank A., Vorstandsvorsitzender der Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn;
2. Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, eingetragen im Handelsregister beim Amtsgericht Bonn HRB 6792;

wegen des Verdachts auf Straftaten nach §§ 44, 43, 6b, 4, 33, 11 BDSG gegen den Verdächtigen zu 1),

verbunden mit der Anregung an die mit gleicher Post verständigte Landesbeauftragte für den Datenschutz Nordrhein-Westfalen, Kavalleriestraße 2-4, 40213 Düsseldorf, vorab per Fax: 0211-38424-10,

jeweils Strafantrag nach §§ 44 Abs. 2 BDSG, 77 Abs. 1, 77d StGB zu stellen,

sowie wegen des Verdachts auf Ordnungswidrigkeiten nach §§ 43, 6b, 4, 33 BDSG gegen die o. g. natürlichen und juristischen Personen. Im Fall des §§ 43, 30, 35 Abs. 6 OWiG, § 43 Abs. 3 Satz 1 BDSG wird Abgabe an die o.g. Landesdatenschutzbeauftragte angeregt.

Die Landesdatenschutzbeauftragte wird hiermit ausdrücklich angeregt,

dem Unternehmen zu 2) die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren nach § 38 Abs. 5 BDSG untersagen.

Begründung:

I. Sachverhalt

Der Verdächtige zu 1) ist Vorstandsvorsitzender eines Post- und Logistikunternehmens mit einem Mitarbeiterstamm von ca. 508.000 Personen, das in seinen Filialen und Partnerfilialen auch Produkte im Einzelhandel anbietet. Dieses betreibt in ihren für die Öffentlichkeit zugänglichen Räumen neben konventioneller Kameraüberwachung zur Wahrung des Hausrechts und von Sicherheitsbelangen auch neuartige Personenscanner mit Gesichtserkennungsfunktion zu Zwecken des Marketings.

Das Unternehmen testet in ca. 100 Partnerfilialen, darunter in NRW etwa in Schreibwarengeschäften in Köln, seit Herbst 2016 ein System des Dienstleisters Corporate Communication AG, Curt-Frenzel-Straße 10, 86167 Augsburg, mit dem das Verhalten von Kunden analysiert wird, die auf Displays eingespielte Werbung betrachten. Eine Kamera über dem Display im Kassenbereich registriert dabei alle Blickkontakte zu dem Bildschirm. Die

aufgenommenen Bilder werden rein automatisch mit einer Software „Adpack“ der Firma Indoor Advertising (IDA) ausgewertet und dann sofort wieder verworfen. Die Bilder befinden nur für jeweils ca. 150 Millisekunden im Speicher und werden weder übertragen noch gespeichert. Die so ermittelten Metadaten, also Anzahl der Betrachter, Geschlecht, Alter und Blickkontakte, werden an die Firma Echion ausgeleitet, die zu diesen anonymen Kundenprofilen dann individuell personalisierte Werbung einspielt. Welche Produktwerbungen aufgrund welcher Kriterien konkret zugeordnet werden, ist hier unbekannt. Außerdem soll der Einsatz auch zur Messung der erhofften Werbewirkung dienen, damit Echion potenziellen Kunden die Wirksamkeit des Mediums "TV in der Kassenzone" schmackhaft machen könne (Kanneberg, Presseartikel „Werbedisplays mit Gesichtserkennung auch in Real-Märkten“, veröffentlicht unter der URL https://www.heise.de/newsticker/meldung/Werbedisplays-mit-Gesichtserkennnung-auch-in-Real-Maerkten-3728931.html, Reinle, Moos, Presseartikel, „Post und Real scannen Kundengesichter für Werbung“ http://www1.wdr.de/nachrichten/gesichtserkennung-personalisierte-werbung-100.html.)

Weder werden die Kunden um eine Einwilligung ersucht noch wäre hier im Hinblick auf die Arbeitnehmer eine entsprechende Betriebsvereinbarung bekannt. Die Betroffenen werden lediglich auf die konventionelle Kameraüberwachung hingewiesen, nicht aber auch auf eine solche mit Gesichtserkennung, intelligenter Datenverarbeitung und Tracking. Den Betroffenen ist daher weder ihre qualifizierte Beobachtung bewusst noch ein Bezug zur eingeblendeten personalisierten Werbung. Ein Benachrichtigung über die Überwachung erfolgt ebenfalls nicht. Eine Möglichkeit, der Beobachtung zu widersprechen, wird mithin verwehrt.

Angeblich speichert das System die erfassten biometrischen Daten und die Verweildauer der Betrachtung nicht und gibt nur die durch Auswertung entstandenen Metadaten verschlüsselt an Echion weiter. Ob die Metadaten auch einen Zeitstempel aufweisen oder ein solcher auch dauerhaft gespeichert wird, ist unklar. Die Verwendung eines Zeitstempels ist allerdings naheliegend, da bei der Generierung entsprechender Datei- oder Feldnamen üblicherweise auf Kalenderdatum und Uhrzeit oder ähnliche Systeme zurückgegriffen wird, die einen Rückschluss auf den Zeitpunkt der Datenerfassung erlauben. Eine weitere Identifizierung der Betroffenen und damit die Zuordnung der Metadaten könnte dann auch nachträglich erfolgen. Möglich wäre dies

etwa durch Abgleich mit Abrechnungsdaten von Kreditkartenzahlung und Rabattsystemen, mit Aufzeichnungen konventioneller Videoüberwachung oder mit Tracking von Produkten z.B. mit RFID-Systemen. Ferner wird in der Werbebranche offen diskutiert, bei Smartphones von Kunden mit eingeschaltetem WLAN die Netzwerkseriennummer des Geräts auszulesen und zu speichern. Technisch wäre dies einfach zu realisieren. Zudem ist auch eine indirekte Speicherung von zusammengeführten Daten vorstellbar, wenn konventionelle Überwachungskameras die Werbemonitore erfassen und damit gleichzeitig auch das Ergebnis der Datenverarbeitungsvorgänge nebst der betroffenen Person aufzeichnen.

Von einer Speicherung der Metadaten bei Echion ist ebenfalls auszugehen, da das System auch der Messung von Werbewirkung dienen soll. Der Nachweis der Effizienz des Systems dürfte auch für die Vergütung der Dienstleisterin erforderlich sein.

Aus den in der Presse bekanntgewordenen Stellungnahmen des Unternehmens und von Landesdatenschützern ist zu schließen, dass der Verantwortliche vorab keine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt hat, wie sie Art. 35 Datenschutzgrundverordnung ab dem 25.05.2018 vorgesehen ist.

II. Strafbarkeit des Verdächtigen zu 1)

Die Verdächtige zu 1) ist Straftaten nach §§ 44, 43, 4, 6b, 33 BDSG verdächtig. Die Erhebung der Daten sowie deren Verarbeitung und Nutzung sind rechtswidrig, da es sich um personenbezogene Daten nach §§ 6b, 3 Abs. 1 BDSG handelt und insoweit weder eine Einwilligung nach § 4a BDSG noch ein rechtfertigendes Interesse gegeben ist, das die Belange des allgemeinen Persönlichkeitsrechts der Kunden überwiegt.

1.
Für die genannte Firma gilt als Privatunternehmen das Bundesdatenschutzgesetz nach § 2 Abs. 4 BDSG und § 1 Abs. 2 Nr. 3 BDSG, da es sich um eine nicht-öffentliche verantwortliche Stelle handelt, § 3 Abs. 7 BDSG. Bei den Verkaufsräumen handelt es sich um öffentlich zugängliche

Räume iSd § 6b Abs. 1 BDSG, vgl. BT-Drs. 14/4329, 38. Im neugefassten § 6b Abs. 1 BDSG werden Einkaufszentren eigens aufgeführt.

2.
Die Erfassung der Kunden mit Kameras, gleichgültig ob verdeckt oder offen, ist eine „Beobachtung“ mit „optisch-elektronischen Einrichtungen“ iSd § 6b Abs. 1 BDSG, da diese mit einer gewissen Dauer erfolgt. Eine Aufzeichnung oder Signalverarbeitung ist hierzu nicht erforderlich (Simitis-Scholz, Bundesdatenschutzgesetz, 8. Auflage 2014, § 5b, Rn. 38, 40). So hat der EuGH in der Sache EuGH (4. Kammer), Urteil vom 11.12.2014 – C-212/13 (Ryneš/Úřad pro ochranu osobních údajů) entschieden, dass jedenfalls das vorübergehende Speichern auf einer automatisch wieder zu überschreibenden Festplatte eine automatisierte Verarbeitung personenbezogener Daten gem. Art. der 3 Abs. 1 EWG RL 95/46 darstellt. Entscheidend ist mithin das Tatbestandsmerkmal der automatisierten Verarbeitung. Auch der bloßen Beobachtung mittels Bildübertragung (sog. Kamera-Monitoring-Prinzip) kommt bereits Eingriffscharakter zu, schon weil damit regelmäßig eine Erhebung personenbezogener Daten verbunden ist, vgl. OVG Hamburg Urteil vom 22.6.2010, 4 Bf 276/07, Rn. 55. Der Umstand, dass das Ergebnis der Observation in Metadaten umgewandelt und damit zumindest gegenüber Dritten anonymisiert wird, lässt die das Tatbestandsmerkmal der Erfassung der Daten durch optisch-elektronischen Einrichtungen nicht nachträglich entfallen. Lediglich reine Kamera-Monitor-Systeme (Beobachtung mittels Bildübertragung) fallen aus dem Anwendungsbereich der Art. 3 Abs. 1 Alt. 2 der Richtlinie heraus, da aufgrund der fehlenden Möglichkeit zur Aufzeichnung von Bild- und Tondaten keine Sammlung der flüchtigen Daten möglich ist (Simitis-Scholz, aaO, Rn. 19; Weichert, DuD 2000, 664; Königshofen, RDV 2001, 221 f.; Lang, S. 216). Auch die Observation durch einen Privatdetektiv wird als Erheben von Daten angesehen, welche Informationspflichten auslöst, EuGH, Urteil vom 07.11.2013 – C-473/12; Kühling-Buchner: Datenschutzgrundverordnung, 1. Aufl. 2017, Art. 13 Rn. 15. Die Kürze der Speicherdauer von angeblich 150 Millisekunden ist für den Begriff der Datenverarbeitung irrelevant, da in diesem Zeitraum ein Vielzahl an Verarbeitungsvorgängen und Abgleichen möglich ist.

Aus der Systematik des BDSG folgt, dass „Beobachten“ nur das Erheben personenbezogener oder personenbeziehbarer Daten ist. Personenbezug ist bereits bei Bestimmbarkeit gegeben (Simitis-

Scholz, aaO, Rn. 67). „Bestimmbarkeit“ einer Person bedeutet in diesem Zusammenhang, dass die von der Überwachung betroffene Person so genau erfasst wird, dass sie mit noch verhältnismäßigem Aufwand identifizierbar ist, gleichgültig, ob für die verantwortliche Stelle eine solche Identifizierbarkeit für alle betroffenen Personen besteht oder angestrebt wird (Wedde, in: DKWW, BDSG, § 6b Rdnr. 13; Roßnagel/v. Zezschwitz, Handbuch, 9.3 Rdnr. 23).

Ein solcher Personenbezug besteht auf mehreren Ebenen:
Eine Identifikation findet bereits gegenüber der beobachteten Person selbst statt, da diese während des Aufenthalts auf der Verkaufsfläche von entsprechenden Kameras identifiziert, mithin getrackt wird. Eine Identifizierung in der Weise, dass eine Person permanent etwa namentlich oder vom Aussehen her identifiziert werden kann, ist nicht erforderlich, vielmehr kommt es auf den Zeitpunkt der Datenverarbeitung an. Mithin ist bereits der Beobachtungsvorgang auf der Verkaufsfläche personenrelevant.
Gegenüber einem insoweit aufgeklärten Kunden, der sich etwa in den Medien über die verdeckte qualifizierte Überwachung informiert hat, ist die Beobachtung auch geeignet, einen nicht unerheblichen Überwachungs- und Anpassungsdruck hervorzurufen und wirkt sich somit als Grundrechtseingriff aus, vgl. Simitis-Scholz, aaO, Rn. 27.
Das identifizierende Beobachten kulminiert zudem in der Konfrontation der betroffenen Person mit dem personifizierten Ergebnis der Auswertung ihres Verhaltens. Unerheblich ist insoweit, ob die betroffene Person die präsentierte Werbung als das Ergebnis eines personenbezogenen Datenverarbeitungsvorgangs wahrnimmt oder ob dieses verheimlicht wird.
Eine solche Identifikation der betroffenen Person mit den zu ihr gesammelten Daten erfolgt auch gegenüber Dritten, welche im Kassenbereich ebenfalls die Ergebnisse der beobachteten Präferenzen wahrnehmen und auf persönliche Interessen schließen können.
Die Pseudonymisierung der Metadaten wäre jedenfalls dann aufgehoben, falls solche mit weiteren Daten abgeglichen oder mit einem Zeitstempel gespeichert werden, wie dies wie oben ausgeführt naheliegend ist.
Anhand der offenbar gespeicherten Metadaten können Besucher möglicherweise auch bei künftigen Besuchen wiedererkannt und zugeordnet werden. So ist etwa im Online-Bereich eingesetzte Software inzwischen in der Lage, nicht eingelogte Nutzer schon anhand ihres Online-

Verhaltens mit einem hohen Grad an Zuverlässigkeit durch Abgleich mit Kunden-Profilen zu identifizieren.
Eine weitere Bestimmbarkeit ergibt sich auch aus der Tatsache, dass die Angestellten wohl ebenfalls erfasst werden, diese allerdings den Verdächtigen namentlich bekannt sind. An die Zulässigkeit für Überwachung von Angestellten legt die Rechtsprechung strenge Kriterien an, vgl. Alter, Maximilian J., NJW 2015, 2375. Ein solcher „Beifang“ wäre ohne individuelle Einwilligung der Betroffenen nur bei Bestehen einer entsprechenden Betriebsvereinbarung zulässig, von einer solchen hier bislang nichts bekannt ist.

3.
Das Erheben, Verarbeiten und Nutzen dieser personenbezogenen Daten ist rechtswidrig, da es an einer Einwilligung oder sonstigen Rechtsgrundlage hierzu fehlt, §§ 4 Abs. 1, 3 Abs. 3, Abs. 4, Abs. 5 BDSG.

Eine Rechtfertigung nach § 28 Abs. 1 Nr. 1 BDSG scheidet aus, da die Erhebung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen vorliegend nicht erforderlich ist. Aktuelle Schuldverhältnisse und deren Abwicklung werden nicht beeinflusst. Der Kaufvertrag zwischen Kunde und Unternehmen wird erst an der Kasse geschlossen. Für vor diesem Zeitpunkt bestehende Schuldverhältnisse wie culpa in contrahendo ist keine Erforderlichkeit des Ausspionierens der Kundeninteressen erkennbar, ebenso wenig beim Vertragsschluss, da im Zeitpunkt der Werbeeinblendung die aktuelle Kaufentscheidung bereits getroffen wurde, die Werbung vielmehr auf künftige Kaufentscheidungen zielt.

Eine Zulässigkeit könnte sich allenfalls aus § 28 Abs. 1 Nr. 2 BDSG ergeben, soweit die Erhebung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.
Als berechtigtes Interesse gilt nicht nur ein rechtliches, sondern bereits jedes tatsächliche Interesse , das wirtschaftlicher oder ideeller Art sein kann, BAGE 127, 276. Es bestimmt sich jedoch nicht allein nach den subjektiven Wünschen und Vorstellungen der verantwortlichen Stelle, sondern

muss objektiv begründbar sein, d.h. sich aus der konkreten Sachlage ergeben. Die Berufung auf einen beliebigen Geschäftszweck ist nicht ausreichend. Wegen Grundrechtsgehalt ist „berechtigtes Interesse“ restriktiv auszulegen (Simitis-Scholz, aaO, Rn. 78).

Ohne Einverständnis der betroffenen Personen ist eine Beobachtung öffentlich zugänglicher Bereiche mit optisch-elektronischen Einrichtungen gemäß § 6b Abs. 1 BDSG durch Private nur zulässig, wenn sie im konkreten Fall zur Wahrung berechtigter Interessen des Überwachenden erforderlich ist und kein überwiegendes Interesse der betroffenen Personen am Schutz ihrer Privatsphäre entgegensteht, BGH, NJW 2013, Rn. 14 f.. Als berechtigte Interessen des Überwachenden erkennen das deutsche und europäische Datenschutzrecht namentlich den Schutz des Überwachenden und anderer Personen vor Eingriffen in Leib, Leben oder Eigentum sowie die Ermöglichung der straf- und zivilrechtlichen Verfolgung solcher Eingriffe an, BGH, NJW 2013, 3089 Rn. 14 f.; OLG Köln, NJW 2005, 2997; Elzer, NJW 2013, 3537, so auch nunmehr Art.6 Abs. 1 d) DSGV. Voraussetzung ist dabei die konkrete Gefahr von künftigen Eingriffen. Ob ein berechtigtes Interesse des Überwachenden oder aber das Interesse der betroffenen Personen am Schutz ihrer Privatsphäre überwiegt, muss durch Abwägung im jeweiligen Einzelfall entschieden werden, vgl. Stöber, Michael, NJW 2015, 3681, vgl. auch Art. 6 Abs. 1 f). Bislang wurden solche Interessen von der Rechtsprechung offenbar nur bei der Gefahrenabwehr anerkannt, vgl. OVG Lüneburg, Urteil vom 29.9.2014 – 11 LC 114/13:

> *(...) Die Interessenprüfung gem. § 6b Abs. 1 und 3 BDSG erfordert 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 sind. Bei der Abwägung sind auf Seiten der verantwortlichen Stelle insbesondere die Zwecksetzung der Beobachtung sowie die sie begleitenden Umstände (vor allem deren technische Ausgestaltung) zu beachten, während auf Seiten der von der Überwachung betroffenen Personen in erster Linie das allgemeine Persönlichkeitsrecht gem. Art. 2 GG Abs. 1 iVm Art. 1 GG, Art. 2 Abs. 1 GG in seinen Ausprägungen als Recht der informationellen Selbstbestimmung, des Rechts am eigenen Bild sowie des Schutzes der Privatsphäre von Bedeutung ist (Zscherpe in Taeger/Gabel, § 6 b Rn. 53; Scholz in Simitis, § 6 b Rn. 23 u. 92, jew. mwN). Hierbei sind alle*

Gesamtumstände des Einzelfalls maßgeblich. Der Frage der Eingriffsintensität kommt eine entscheidende Bedeutung zu. Das Gewicht des Eingriffs wird 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. Je stärker das Maß der Beeinträchtigung durch die Überwachungsmaßnahme ist, desto schutzwürdiger sind die Interessen der betroffenen Personen. Hinsichtlich des allgemeinen Persönlichkeitsrechts ist zwischen drei Sphären zu unterscheiden, innerhalb derer das Persönlichkeitsrecht betroffen sein kann: die Individualsphäre, die Privatsphäre und die Intimsphäre (zu dieser Unterscheidung vgl. etwa LG München I, Urt. v. 21.10.2011 – 10 O 19879/10, BeckRS 2012, 4221 mwN). Ein Überwiegen der Interessen der Betroffenen muss dabei nicht positiv festgestellt werden, es reicht aus, wenn Anhaltspunkte für ein Überwiegen dieser Interessen nicht ausgeräumt sind (Scholz in Simitis, § 6 b Rdrn. 92 ff. mwN). Dabei ist zu berücksichtigen, dass nach der Wertung des Gesetzgebers die Videoüberwachung und -Speicherung auch durch nicht-öffentliche Stellen im öffentlich zugänglichen Bereich zu den genannten – hier gegebenen – Zwecken grundsätzlich zulässig ist und „lediglich" unter dem genannten Vorbehalt steht. (...)

Vorliegend wäre eine Überwachung nur dann zulässig, wenn das Interesse des Werbetreibenden an der Optimierung seiner Kundenansprache ausreicht und die das Recht auf informationelle Selbstbestimmung der Käufer überwiegt. Das Interesse eines Werbetreibenden tangiert die Gewerbefreiheit, die in Art. 12 GG grundrechtlich geschützt ist. Mithin kollidiert dieses Grundrecht mit dem allgemeinen Persönlichkeitsrecht, das in Art. 2 Abs. 1, Art. 1 GG ebenfalls Grundrechtsrang genießt.

Zwar ist nicht grundsätzlich auszuschließen, dass einzelnen Kunden die aufgedrängte personalisierte Werbung als Empfehlung erwünscht ist. Die Intensität des Eingriffs relativiert sich auch insoweit, als dass ein Kunde an der Ladentheke den Großteil seiner Präferenzen ohnehin durch öffentlich wahrnehmbares Handeln preisgibt, in dem er Waren aufs Fließband legt.

Allerdings sind Fälle vorstellbar, in denen eine jedenfalls für Dritte wahrnehmbare Preisgabe von Interessen definitiv unerwünscht ist:

So wähnen sich Kunden unbeobachtet, wenn sie etwa Hygiene-Artikel mit Sexualbezug inspizieren. Ebenfalls problematisch wäre die Zuordnung beim Ansehen von Zeitschriften-Covern. So könnte eine Software hieraus Rückschlüsse auf sexuelle Orientierung, politische Einstellungen und religiöse Überzeugungen folgern, auch wenn die entsprechende Publikation gar nicht in den Warenkorb gelangt und damit willentlich offengelegt würde. Gem. Art. 8 Abs. 1 der Richtlinie 95/46/EG ist sicherzustellen, dass aus der Überwachung nicht auf die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder Gesundheit oder Sexualleben gefolgert werden kann.

Im Bereich des Online-Trackings ist es bereits vorgekommen, dass eine intelligente Software aus dem Käuferverhalten zutreffend auf eine Schwangerschaft einer minderjährigen Bestellerin schloss, welche durch Glückwünsche dem Vater bekannt wurde.

Fragwürdig wäre auch die gezielte Bewerbung von Kindern etwa mit Süßigkeiten, was am in Art. 6 GG geschützten Grundrecht der Eltern und am Staatsziel des Jugendschutzes zu messen wäre, das u.a. im Anhang zu § 3 Abs. 3 UWG Nr. 28 Niederschlag gefunden hat. Insbesondere in Art. 6 Abs. 1 f) DSGV, der die Abwägung zwischen berechtigten Interessen und dem allgemeinen Persönlichkeitsrecht, betrifft, werden Kinder eigens aufgeführt.

Auch triviale Anliegen wie das Verbergen von Interesse an nicht-veganen Lebensmitteln gegenüber einem entsprechend orientierten Lebenspartner oder Vorliebe für Schweinefleisch-Produkte gegenüber Begleitern, die solches aus religiösen Überzeugungen ablehnen, sind grundsätzlich vom allgemeinen Persönlichkeitsrecht geschützt. Ferner ist denkbar, dass das System biometrisch ein körperliches Geschlecht erkennt, das eine Person wegen anderer sexueller Identifikation verbergen möchte.

Schon heute kann die Technik nicht nur Alter und Geschlecht, sondern auch Emotionen vom Gesicht ablesen. Ein weiterer Schritt wäre die Analyse der Bekleidung, um auf die Kaufkraft der Kunden zu schließen, vgl. Stern-Artikel vom 31.05.2017, http://www.stern.de/wirtschaft/news/real-analysiert-die-gesichter-der-kunden---doch-das-ist-erst-der-anfang-7474404.html. Es ist zudem nur eine Frage des Fortschritts der Technik, bis nicht nur das Betrachten des Displays mit einem gefilterten Werbeangebot, sondern auch der gesamte Besuch der Verkaufsfläche erfasst werden kann, etwa das Verweilen vor Regalen mit jeglichen Artikeln, was den Grad an offenbarten Präferenzen dramatisch erhöhen würde.

Demgegenüber ist das Interesse des Werbetreibenden an der Optimierung seiner Kundenansprache jedenfalls nicht so gewichtig, als dass diesem nicht zuzumuten wäre, das jeweilige Einverständnis seiner Kunden einzuholen. Ein solches ließe sich durch biometrische Scanner einfach bewerkstelligen, etwa durch Heben oder Senken eines Daumens vor einem entsprechenden Hinweisschild. Für eine solch niedrige Gewichtung der Werbeinteressen spricht auch der Vergleich mit den Sicherheitsbelangen, die im neu gefassten § 6b BDSG als gewichtige Interessen eingefügt wurden. Insoweit hat der Gesetzgeber im Videoüberwachungsverbesserungsgesetz vom 28.04.2017, welches Art. 6 Abs. 1 d) DSGV umsetzte, keine anderen Erwägungen erkennen lassen. Solche wurden auch in der Begründung im entsprechenden Referentenentwurf vom 24.11.2016 des Bundesinnenministeriums nicht einmal diskutiert, obwohl die Technologie zu diesem Zeitpunkt der Fachwelt bekannt war, vielmehr hatte der Gesetzgeber der Videoüberwachung einzig den Aspekt der Gefahrenabwehr beigemessen.

4.
Die genannten Verstöße gegen § 6b BDSG sind nach §§ 44, 43 Abs. 2 Nr. 1, 3 und 4 BDSG für den Verdächtigen zu 1) strafbar, auch wenn § 6b BDSG nicht eigens in § 43 Abs. 2 BDSG aufgeführt ist, vgl. Simitis-Scholz, aaO Rn. 159.

Die Beteiligten handelten bzw. handeln in Bereicherungsabsicht nach § 44 Abs. 1 BDSG, da insoweit erforderliche Fremdbereicherungsabsicht zugunsten der Unternehmen insoweit ausreichend ist. Die Verdächtigen handelten vorsätzlich und schuldhaft. Ein Irrtum über die Strafbarkeit wäre wegen Fahrlässigkeit unbeachtlich, § 17 StGB.

5.
Zu einem hier erforderlichen Strafantrag ist neben von der Überwachung konkret Betroffenen auch die Landesdatenschutzbeauftragte als zuständige Aufsichtsbehörde berechtigt, § 44 Abs. 2 BDSG. Auf die Frist in § 77d StGB wird hingewiesen.

III. Ordnungswidrigkeiten

Der Verdächtige zu 1) sowie das Unternehmen zu 2) haben sich daneben der Begehung von Ordnungswidrigkeiten § 43 Abs. 1 und 2 BDSG verdächtig gemacht.

1.
Die unter II. genannten Handlungen sind als Ordnungswidrigkeiten nach § 43 Abs. 1 und 2 BDSG zu qualifizieren.

Aufgrund der schwerwiegenden Verstöße, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, ist gemäß § 38 Abs. 5 BDSG die Erhebung, Verarbeitung oder Nutzung oder der Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden.

2.
Ungeachtet der Frage der Rechtswidrigkeit der datenverarbeitenden Videoüberwachung als solcher verletzen die Beteiligten auch Ihre Informationspflichten diesbezüglich nach § 6b Abs. 2 BDSG.

Die Überwachung von Geschäftsgebäuden wie den Verkaufsflächen (zur Gefahrenabwehr) wird dann als zulässig angesehen, wenn die Besucher beim Betreten hierauf nach § 6b Abs. 2 BDSG hingewiesen werden, OVG Lüneburg, Urteil vom 29.9.2014 – 11 LC 114/13, BayObLG, NJW 2002, 2893; vgl. auch AG Berlin-Mitte, NJW-RR 2004, 532 f.). Vorliegend ist unklar, ob § 6b Abs. 2 BDSG selbst verletzt ist, da die Vorschrift lediglich aufgibt, den Umstand der Beobachtung in ausreichender Weise kenntlich zu machen. Der Begriff „Umstand“ beinhaltet die Tatsache, dass eine Überwachung mit Kameras erfolgt, nicht aber muss auch die Art und Weise der Beobachtungsmaßnahmen kenntlich gemacht werden. Anders als in anderen Vorschriften des BDSG hat der Gesetzgeber auch nicht ausdrücklich aufgegeben, dass insoweit auch Zweck der Überwachung kenntlich gemacht werden muss, so dass aus dem Wortlaut des Abs. 2 keine entsprechenden Pflichten hergeleitet werden können. Allerdings muss der Betroffene, der nicht nach § 4a BDSG in eine Beobachtung eingewilligt hat, nach § 6b Abs. 4 BDSG entsprechend § 33 Abs. 1 BDSG über eine Datenverarbeitung oder -Nutzung benachrichtigt werden, wenn durch die Videoüberwachung erhobene Daten seiner Person zugeordnet werden. Eine Ausnahme nach § 33

Abs. 2 BDSG ist nicht ersichtlich. Auch eine durch systematische Auslegung gewonnene Beschränkung des Anwendungsbereichs auf gespeicherte Daten (Simitis-Scholz, aaO Rn. 133) käme vorliegend zum gleichen Ergebnis, wenn die einer Person zuordbaren Metadaten gespeichert werden. Ebenso wenig folgt aus dem Schweigen von § 6b Abs. 2 BDSG, dass insoweit nachträgliche Informationspflichten entfallen, vielmehr zielt die Vorschrift ersichtlich auf Gefahrenabwehr bekannt, die vom Kunden prinzipiell akzeptiert werden muss, während mit einer qualifizierten automatischen Auswertung der Käuferpräferenzen nicht gerechnet werden muss. Mithin ist der Zweck der Beobachtung spätestens im Zeitpunkt der Datenerhebung bekannt zu geben. Dem jedoch genügen Piktogramme mit dem Hinweis auf konventionelle Kameraüberwachung nicht. Eine unterlassene Benachrichtigung nach § 33 Abs. 1 BDSG ist nach § 43 Abs. 1 Nr. 8 BDSG mit Bußgeld von bis zu 300.000,- € bewehrt.

3.

Es bestehen Zweifel, ob das Verfahren automatisierter Datenverarbeitung vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde gemäß § 4d BDSG gemeldet wurde. Außerdem enthält der – wenn auch erst ab dem 25.05.2018 anzuwendende - Art. 35 Abs. 1, Abs. 3 DSGV die Auflage einer Datenschutz-Folgenabschätzung, die insbesondere in folgenden Fällen für erforderlich ist:

1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 oder
3. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

An einer solchen Datenschutz-Folgenabschätzung fehlt es nach hiesigem Kenntnisstand bislang.

Mit freundlichen Grüßen

Markus Kompa
Rechtsanwalt