Quelle: iStock.com/LeoWolfert

/// IM ZEITGESPRÄCH:
GERALD SPYRA, LL.M.

ist Rechtsanwalt, externer betrieblicher Datenschutzbeauftragter und Partner in der medizinrechtlichen Sozietät RATAJCZAK & PARTNER mbB, Köln.

/// Meine Daten gehören mir!

BRAUCHEN WIR MEHR ODER WENIGER DATENSCHUTZ?

Datenschutz ist kein Selbstzweck. Er soll in einer vernetzten Informationsgesellschaft dem Ausufern staatlicher Überwachungsmaßnahmen und der Entstehung von Datenmonopolen von Privatunternehmen entgegenwirken. Ziel aller datenschutzrechtlichen Regelungen ist es, das Grundrecht auf informationelle Selbstbestimmung zu gewährleisten. Aber wie ist die Realität? Gibt es zu viel oder zu wenig Datenschutz? Wir haben mit dem Rechtsanwalt und Datenschutzexperten Gerald Spyra über diese Fragen diskutiert.

Politische Studien: Herr Spyra, finde ich Sie auf Facebook, auf Instagram oder Twitter und kann ich Ihnen eine Nachricht per WhatsApp schreiben?

Gerald Spyra: Nein. Ich nutze diese Dienste nicht und daher können Sie mir auch keine „Nachricht" schreiben. Denn die Risiken, die mit diesen Diensten einhergehen, übersteigen den Nutzen, den ich aus ihnen ziehen kann. Leider wollen viele Menschen aber nur den Nutzen sehen, jedoch sich nicht mit den Risiken auseinandersetzen. Insofern kann man dort sehr gut eine sogenannte kognitive Dissonanz beobachten. Spricht man die Nutzer auf die Risiken an, hört man oft: „Da kann man doch nix ändern, das machen doch alle." oder „Man kann gar nicht mehr ohne!". M. E. n. kann man aber sehr gut auch ohne diese Medien auskommen und fördert damit sogar das Persönliche. Auch das Argument „Das hat doch jeder" kann ich so nicht stehenlassen. Denn jeder hat auch Karies. Ist Karies deshalb gesund? Es ist absolut essenziell, sich mit der ganzen Digitalisierungsthematik offen und ehrlich auseinanderzusetzen und dabei Nutzen und Risiken abzuwägen. Man darf diese Medien in keinem Fall als „alternativlos" betrachten.

Wer sich mit US-Amerikanern unterhält, trifft häufig auf Unverständnis, wenn wir als Deutsche unsere Idee von Datenschutz erläutern. Täuscht dies oder beobachten Sie in Deutschland ein besonders hohes Maß an Datensensibilität?

Das (noch) unterschiedliche Verständnis beim Datenschutz dürfte u. a. aus unserer unterschiedlichen Vergangenheit herrühren. In Deutschland haben wir gesehen und erleben müssen, was etwaige Auswirkungen sein können, wenn Kenntnisse, beispielsweise über eine „falsche" Gesinnung, Religion, sexuelle Orientierung usw. in falsche Hände geraten. Leider beobachte ich in Deutschland, dass durch den erfolgten Generationenwechsel immer weniger Sensibilität für den Schutz von Daten vorhanden ist. Wir gleichen uns vielmehr immer mehr dem amerikanischen Mindset an, was ich für sehr bedenklich halte. Die deutsche Generation der sogenannten Digital Natives wächst mit IT auf und nutzt diese. Sie reflektieren aber oftmals nicht über die Risiken, die damit einhergehen. Gerade dies ist jedoch notwendig, um IT verantwortungsbewusst nutzen zu können und Maßnahmen zu ergreifen, um den Nutzen von IT mit den Risiken in ein angemessenes Verhältnis zu bringen.

> Viele glauben, von diesen Unternehmen nichts befürchten zu müssen und ahnen nicht, dass Staaten und diese Unternehmen **KOOPERIEREN**.

Viele Bürger haben Angst vor staatlicher Überwachung, geben aber trotzdem bereitwillig Daten an soziale Netzwerke oder Online-Händler aus den USA oder gar China weiter. Was sagen Sie zu diesem ambivalenten Verhalten?

Dieses Verhalten ist nicht verwunderlich und hängt mit unserer Vergangenheit zusammen. Der Staat ist in den Köpfen vieler Bürger der „Große Bruder", der sie überall überwachen will. Diese Bedenken sind ja auch nicht ganz unbegründet, insbesondere, wenn man Länder wie China oder die USA betrachtet. Außerdem sollte man auch den psychologischen Aspekt von „Geschenken" nicht außer Acht lassen. Der Staat schenkt den Bürgern nichts. Von den Dienstleistern bekommen die Menschen aber etwas „geschenkt", z. B. eine „kostenlose" Kommunikationsmöglichkeit durch Facebook, Google oder WhatsApp. Viele glauben, von diesen Unternehmen nichts befürchten zu müssen, doch sie ahnen oftmals nicht, dass Staaten und diese Unternehmen miteinander kooperieren. Aufgrund dieser Kooperation ergeben sich für den Bürger nun von beiden Seiten „Risiken", die er sorgfältig betrachten und bei der Nutzung berücksichtigen sollte.

Am 25. Mai 2018 trat die 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 in Kraft. Wir kennen dieses Regelwerk besser unter dem Namen Datenschutz-Grundverordnung oder kurz DSGVO. Die Verordnung hat vor drei Jahren für ziemlich Unruhe in der Öffentlichkeit gesorgt. In ihrer ersten Evaluierung der EU-DSGVO vom Mai 2020 kritisiert die EU-Kommission Defizite bei der Umsetzung der Datenschutzregeln. Dabei schlägt sie keine wesentlichen Regeländerungen vor, sondern erwartet von den Mitgliedsstaaten eine einheitliche und konsequente Umsetzung der Verordnung. Inzwischen sind fast drei Jahre seit Einführung der DSGVO vergangen. Wie sieht ihr aktuelles Zwischenfazit aus?

Gerade in der jetzigen Zeit beobachte ich ein sehr ambivalentes Verhältnis bei den datenschutzrechtlichen Verantwortlichen. Sie wissen, dass es „Datenschutz" gibt, wollen aber am liebsten nichts (mehr) davon wissen. Gerade bei Unternehmen stehen jetzt ganz andere Themen im Fokus, z. B., wie man diese schwierigen Zeiten wirtschaftlich überhaupt noch überleben

kann. Zudem wissen die Unternehmen oftmals auch gar nicht, was sie alles in Sachen Datenschutz machen sollen. Sie sehen den zu betreibenden Aufwand als unproportional zum Nutzen und meinen, dass Datenschutz nur kostet. Aus Kostengründen oder aufgrund der faktischen Umstände, werden Unternehmen darüber hinaus immer mehr in digitale Technologien getrieben, mit denen der Datenschutz so, wie sich das die DSGVO vorstellt, praktisch nicht umsetzbar ist. Das kann man sehr gut gerade bei den „kostenlosen" Videokonferenzsystemen beobachten, die man gezwungen ist, für die Heimarbeit einzusetzen.

Ein Ziel der DSGVO war es, das Recht EU-weit zu vereinheitlichen. Es wird kritisiert, dass die über 70 Öffnungsklauseln in der DSGVO, durch die Gesetzgeber der Mitgliedsstaaten die Befugnis zugesprochen wird, das Regelwerk zu konkretisieren, eine neue Fragmentierung zugelassen haben. Was ist Ihre Einschätzung dazu?

Es wurde immer gesagt, eine Datenschutz-Richtlinie (RL), die vom nationalen Gesetzgeber in nationales Recht umgesetzt werden muss, schafft keine Einheitlichkeit. Daher wurde die RL durch die DSGVO ersetzt, die direkt und unmittelbar gelten soll. Doch durch die in der DSGVO enthaltenen Öffnungsklauseln wurde diese Einheitlichkeit wieder ausgehebelt. Wir haben damit faktisch eine Richtlinie im Gewand einer Verordnung. Die Auswirkungen spüre ich in meiner Beratungspraxis, etwa bei der Beurteilung einer Datenübermittlung von Land A nach Land B. Wegen der unterschiedlichen Regelungen in den Ländern ist ein solcher Datenaustausch nicht ohne eine gewisse Rechtsunsicherheit realisierbar. Auch diese Rechtsunsicherheit führt letzten Endes dazu, dass der Datenschutz immer weniger ernst genommen wird und nicht die Stellung eingeräumt bekommt, die er mit zunehmender Digitalisierung eigentlich erhalten müsste.

Welchen konkreten Verbesserungsbedarf sehen Sie an der DSGVO?

Die DSGVO beinhaltet viele Regelungen, die schon in die richtige Richtung gehen, auch wenn sie sehr sperrig sind. Insbesondere das Prinzip „Datenschutz by Design" ist ein zielführender Ansatz für das 21. Jahrhundert. Leider adressiert er nur unzureichend diejenigen, die es eigent-

> Der grundsätzliche Umgang mit IT und die diesbezügliche, absolut **INTRANSPARENTE** Datenverarbeitung erfordern ein Umdenken.

> Die Unternehmen wissen oftmals gar nicht, was sie in Sachen **DATENSCHUTZ** machen sollen.

lich angeht. Die großen Softwarehersteller werden davon oftmals nicht bzw. unzureichend erfasst. Vielmehr trifft es die Unternehmen, die die Software einsetzen wollen. Es sind m. E. n. aber eher weniger die gesetzlichen Regelungen, die geändert werden sollten. Es sind vielmehr der grundsätzliche Umgang mit IT und die diesbezügliche, absolut intransparente Datenverarbeitung, die ein Umdenken erfordern. Es fehlen oftmals auch entsprechende Haftungsregelungen, was zu Rechtsunsicherheiten führt. Denn, auch wenn man das nicht glauben mag, haften die Softwarehersteller oftmals nicht für Fehler in ihrer Software, wenn sie zeitnah die Lücke geschlossen haben.

Sie sind externer betrieblicher Datenschutzbeauftragter und beraten Unternehmen. Wie ist es zu erklären, dass sich immer noch viele Organisationen wie Vereine, aber auch Unternehmen schwer damit tun, die Datenschutz-Grundverordnung umzusetzen?

Wie gesagt, die DSGVO ist sehr sperrig und selbst für Juristen schwer zu verstehen, weshalb viele Regelungen bzw. deren Umsetzung gerade für kleine Vereine und Unternehmen übertrieben und unverhältnismäßig erscheinen. Als Vorstand eines Vereins übernimmt man jedoch die Verantwortung für die Daten der Mitglieder. Dazu gehört zwangsläufig, dass man bei der Datenverarbeitung mittels IT stets den Respekt gegenüber dem Betroffenen bewahrt, genauso wie man es im Zwischenmenschlichen tun würde. Daher darf man beispielsweise auch nicht ungefragt „Fremden" wie Google und Co. Interna über die Mitglieder mitteilen. Zur Wahrung dieses Respekts und des Datenschutzes sollten Vereinsvorstände daher so wenig („kostenlose") IT wie möglich einsetzen, denn diese kommerzialisiert zumeist die Daten der Mitglieder. Je weniger, umso geringer ist auch die Gefahr, dass man gegen die Regelungen der DSGVO verstößt. Bei all dem gilt es stets, das richtige Augenmaß zu wahren.

Seit dem 25. Mai 2018 gilt also die DSGVO. Und mit ihr sollte ursprünglich auch die ePrivacy-Verordnung (ePVO) erscheinen. Manche stemmen die Aufgabe DSGVO mit Bravour, andere hinken noch gewaltig hinterher. Doch nun klopft mit der ePVO schon das nächste Datenschutzthema an die Tür. Was hat es damit auf sich und warum braucht es so viele Datenschutz-Regelwerke?

> Ob man die zusätzlichen Regelungen der ePVO braucht, wage ich stark zu **BEZWEIFELN**.

Zunächst glaube ich, um ehrlich zu sein, dass keiner die DSGVO mit Bravour stemmt. Denn die DSGVO-Anforderungen sind mit unserer heutigen IT und der damit einhergehenden intransparenten Datenverarbeitung praktisch nicht zu erfüllen. Gerade weil sich das virtuelle Leben heutzutage immer mehr mittels APPs und Webseiten abspielt und diese eine ganz besondere (wirtschaftliche) Bedeutung einnehmen, sieht es die EU-Kommission als notwendig an, spezielle Regelungen wie die ePVO zu etablieren, die neben denen der DSGVO Anwendung finden. Die ersten Vorboten der ePVO sind die „beliebten" Cookie-Banner, die nun praktisch jede Webseite zieren. Ob man die zusätzlichen Regelungen der ePVO braucht, wage ich stark zu bezweifeln. Doch man merkt durch sie, dass diesem Sektor eine sehr hohe wirtschaftliche Bedeutung zukommt, weshalb auch der Lobbyeinfluss im Gesetzgebungsverfahren und das ständige Verschieben der ePVO-Einführung nicht überraschen dürften.

Neben den angesprochenen Regelungen gab es 2020 auch noch ein wichtiges „Datenschutz-Urteil". Der Europäische Gerichtshof (EuGH) hat am 16. Juli 2020 die Rechtsgrundlage für die Datenübermittlung in die USA gekippt. Das sogenannte „Privacy Shield" ermöglichte bislang vielen Unternehmen in der EU, personenbezogene Daten von Kunden, Mitarbeitern oder auch für die Nutzung von Internetdiensten in die USA zu transportieren und dort verarbeiten zu lassen. Warum wurde das verboten?

Beim Privacy Shield handelt es sich um eine Lösung für amerikanische Unternehmen, Daten von europäischen Bürgern in Amerika zu verarbeiten. Es war praktisch nur eine Registrierung bei einer amerikanischen Behörde notwendig, verbunden mit dem Versprechen, gewisse „Datenschutzregelungen" einzuhalten. Dadurch wurde (gesetzlich) vermutet, dass die Datenverarbeitung sicher und EU-rechtskonform erfolge. Doch es wurden immer mehr amerikanische Regelungen bekannt, die den Zugriff von amerikanischen Behörden auf diese Daten gestatteten bzw. vorsahen. Damit war es faktisch nicht mehr möglich, ein ausreichendes Datenschutzniveau zu gewährleisten, weshalb der EUGH diese Regelung auch einkassiert hat. Damit dürfte es nun immer schwerer werden, Daten aus Europa amerika-

nischen Unternehmen zu übermitteln. Dass der Wegfall dieser Regelung derzeit aber keine große Rolle spielt, sieht man jedoch daran, dass Unternehmen nicht weniger, sondern eher mehr Software-Produkte amerikanischer Unternehmen einsetzen.

Der Mittelstand in Deutschland sieht sich wegen dieses Urteils und generell wegen der strengeren Datenschutzbestimmungen im Wettbewerbsnachteil. Was entgegnen Sie diesem Einwand?

Ja, man kann durch den Datenschutz nicht jede gewünschte Datenverarbeitung durchführen und darin durchaus einen Wettbewerbsnachteil sehen. Doch ist diese Sichtweise nicht zielführend. Denn der Datenschutz ist eine der letzten Bastionen, um den Leuten noch ein wenig die Bedeutung des Respekts vor dem Anderen aufzuzeigen. Vielleicht sollte man sich daher eher fragen, ob die allgegenwärtige Digitalisierung der richtige Weg ist, den die Gesellschaft einschlägt. Denn dabei besteht die Gefahr, dass wir immer mehr entmenschlichen sowie immer mehr die Kontrolle abgeben. Es besteht das Risiko, dass das, was das Menschsein eigentlich ausmacht, immer mehr in den Hintergrund tritt und der Mensch immer mehr zu einer „Nummer" wird. Wenn man diesen Weg nicht will, sollte man sich schnellstens überlegen, wie man IT entwickelt, die den Menschen respektiert und für den Menschen da ist. Denn daraus kann man dann wirklich einen Wettbewerbsvorteil generieren und damit eine Win-Win-Situation erreichen.

Das Jahr 2020 stand ganz im Zeichen der Corona-Pandemie. Vieles musste abgewogen werden. Manchmal, so schien es, auch Datenschutz und Gesundheit. Tracking und Tracing waren in aller Munde. Dürfen wir in der Corona-Krise Abstriche beim Datenschutz machen?

Die Corona-Krise führt immer mehr dazu, dass der Datenschutz wie weggeblasen erscheint. Für viele geht es ums Überleben und da ist der Datenschutz bzw. der Respekt vor dem Anderen erst einmal zweitrangig. Das Problem ist jedoch, dass ein Datenverlust nicht heilbar ist und damit die Risiken für die Betroffenen in Zukunft immer mehr steigen. Die Corona-Krise bietet jedoch die Möglichkeit, wieder zu sich zu finden bzw. sich wieder auf sich zu besinnen und seine Werte zu hinterfragen. Vielleicht hinterfragt man dabei auch mal, ob diese ganze IT, die wir so tagtäglich einsetzen, uns auch wirklich nützt oder ob sie uns nicht immer mehr beherrscht und steuerbar macht. Vielleicht sollte man sich im Sinne eines digitalen Minimalismus auf das reduzieren, was für einen wirklich sinnvoll ist und das andere „gehen lassen". Wir bekommen dann die Möglichkeit, das Geschenk des Lebens und die Chancen, die dieses Leben bietet zu erkennen und einen für uns stimmig anfühlenden Weg zu gehen.

Die Fragen stellte Karl Heinz Keil, Leiter des Referats für Medien, Digitale Gesellschaft, Mobilität, Innovation im Institut für Politische Bildung, Hanns-Seidel-Stiftung, München. ///