Fruzsina Molnár-Gábor und Andreas Merk

16. Spotlight: Die datenschutzrechtliche Bewertung von Neurodaten

Der folgende Kurzbeitrag widmet sich der Frage, welche besonderen Eigenschaften Neurodaten[1] auszeichnen und wie diese Eigenschaften ihre datenschutzrechtliche Bewertung beeinflussen. Neurodaten ergeben sich aus der Messung von Signalen im Gehirn. Häufig werden sie anhand von Gehirn-Computer-Schnittstellen (Brain-Computer-Interfaces, BCIs) durch Sensoren am oder im Kopf ermittelt. Diese Signale werden mithilfe eines Computers in Befehle für ein Programm umgewandelt und interpretiert, sodass der Betroffene mit dem Computer bzw. Programm interagieren kann.[2] Das Anwendungsfeld ist denkbar weit. Es reicht vom Verbraucherkontext wie dem Bedienen eines Kinderspielzeugs oder Computerspiels (Kinney-Lang et al., 2020) bis hin zu medizinischen Anwendungen im Rahmen der Behandlung von Patienten mit physischen Einschränkungen (z. B. Locked-in-Syndrom, ALS-Patienten), insbesondere der digitalen Sprechermöglichung oder anderer technischer Hilfsmittel (Milekovic et al., 2018). Je nach Anwendungskontext können die unterschiedlichen Interessenlagen eine rechtliche Bewertung erheblich beeinflussen, insbesondere Ergebnisse von Abwägungen. Nachstehend soll der Fokus auf medizinischen Anwendungen liegen.

1 Der Begriff „Neurodaten" wird nachstehend wie folgt verwendet: „Daten, die sich auf die Funktionsweise oder Struktur des menschlichen Gehirns einer identifizierten oder identifizierbaren Person beziehen und einzigartige Informationen über ihre Physiologie, Gesundheit oder mentalen Zustände enthalten" (OECD, 2020; Übersetzung durch die Autoren). Nachfolgend wird hinsichtlich des Grades der Sensibilität keine Unterscheidung getroffen zwischen Daten, die sich auf die Funktionsweise des Gehirns beziehen und solchen, die sich auf die Struktur beziehen.

2 Aus der Fülle der Anwendungen, um nur wenige Beispiele herauszugreifen vgl. z. B.: Leeb/Pérez-Marcos (2020); Chaudhary et al. (2016); Chaudhary et. al. (2017); Wang et al. (2019).

16.1 Die Einordnung von Neurodaten in bestehende Kategorien

Daten können in einem weiten Sinne als Analysematerial definiert werden (Taylor, 2012: 41). Personenbezogene Daten, die in den Anwendungsbereich der datenschutzrechtlichen Regelungen wie die der Datenschutz-Grundverordnung (DS-GVO) fallen, beziehen sich auf eine identifizierte oder identifizierbare Person (Art. 4 Nr. 1 DS-GVO). Daten, die vom Gesetzgeber als sensibel und daher besonders schutzwürdig erachtet wurden, sind in einem nicht abschließenden Katalog des Art. 9 Abs. 1 DS-GVO aufgezählt. Hierzu gehören u. a. genetische Daten (Art. 4 Nr. 13 DS-GVO) und Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO). Die allgemeinen Regeln zu personenbezogenen Daten und die spezielleren Vorgaben zu den sensiblen Daten nach Art. 9 Abs. 1 DS-GVO zielen auf den Schutz der Rechte und Freiheiten der betroffenen Personen ab. Welche Beeinträchtigungen durch eine Datenverarbeitung für die Betroffenen entstehen können, hängt wesentlich von den Informationen ab, die mithilfe der Datenanalyse durch Interpretation gewonnen wurden (siehe auch Winkler/Prainsack, Kap. 17). Die erhaltenen Informationen und damit der Grad der Sensibilität der Daten sind kontextabhängig: Eine Kombination und „Kontextualisierung" (Purtova, 2018) gesammelter Daten kann nicht nur das Risiko eines Rückschlusses auf die betroffene Person, sondern auch die Intensität der sich daran anschließenden Beeinträchtigungen ihrer Rechte und Freiheiten zusätzlich erhöhen. Die Verarbeitung von Neurodaten wird im europäischen Datenschutzrecht nicht ausdrücklich geregelt. Unklar ist, ob Neurodaten lediglich als personenbezogene Daten anzusehen sind, als sensible Daten einer in Art. 9 Abs. 1 DS-GVO genannten Kategorie oder als eine neue Kategorie nach Art. 9 Abs. 1 DS-GVO.

Am nächsten erscheinen Neurodaten den Gesundheitsdaten. Diese liefern Informationen über die körperliche oder geistige Gesundheit einer Person. Neurodaten vermögen solche Informationen indirekt auch zu vermitteln, so können bspw. verzögerte neuronale Reaktionsmuster auf Parkinson hindeuten. Allerdings finden neuronale Aktivitäten zwar im menschlichen Körper statt, sie knüpfen aber an den (Gesundheits-) Zustand des Menschen anders an. Sie vermitteln keine mit herkömmlichen Gesundheitsdaten vergleichbaren Informationen über körperliche oder kognitive Eigenschaften des Betroffenen, sondern treffen vielmehr Aussagen über mentale Prozesse, die bewusst oder unbewusst stattfinden (Lavazza, 2018: 3 f.). Inwiefern dieser spezifische Informationsgehalt von Neurodaten eine besondere Nähe zur Identität und Persönlichkeit des Menschen darstellt und ihnen im Vergleich zu anderen sensitiven Daten eine

besondere Qualität verleiht, wird fortlaufend diskutiert.[3] Neurodaten geben Aufschluss über das kognitive System der betroffenen Person. Unklar ist, inwieweit diese Erkenntnisse über den Ursprung des menschlichen Denkens einen Zugriff auf die geistige Blaupause einer Person eröffnen. Aufgrund ihres prädiktiven Potenzials könnten sie also eher mit genetischen Daten vergleichbar sein (Moos, 2011: 217 ff.), denn das Aktivitätsmuster von Neuronen bildet nicht nur einzelne Informationen ab, sondern Muster und Strukturen des Denkens, die eine Bedeutung für das Handeln der Person insgesamt haben können. Hinsichtlich des prädiktiven Potenzials unterscheiden sich Neurodaten allerdings in zwei Punkten wesentlich von genetischen Daten. Erstens kann das prädiktive Potenzial von Neurodaten zu einem deutlich höheren Grad nutzbar gemacht werden. Bei der Ergänzung menschlicher kognitiver Fähigkeiten durch BCI-Technologien können Daten in sehr enger zeitlicher Abfolge in einem ersten Schritt analysiert und in einem zweiten Schritt hirnstimulierend verändert werden. Zweitens sind Neurodaten aufgrund sogenannter kognitiver Verzerrungen, etwa wegen eines unsicheren Informationsgehalts (Hermstrüwer, 2016: 94 ff.) oder eines unsicheren Informationseffekts (ebd.: 113 ff.), stärker von informationellen Unsicherheiten geprägt als genetische Daten oder Gesundheitsdaten. Dies spricht ebenso für die Annahme einer neuen Kategorie von sensiblen Daten nach Art. 9 Abs. 1 DS-GVO.

Die Verarbeitung von Neurodaten kann in Gesundheitskontexten einen erheblichen Beitrag dazu leisten, dass Patienten einen Grad an Autonomie und Handlungsfreiheit erfahren dürfen, der ohne diese Verarbeitung nicht vorstellbar wäre. Mit dem Angebot der Technik geht die Verantwortung einher, nachteilige Folgen für die Personen abzuschätzen und ihnen vorzubeugen.

Hierzu gehört die mögliche Gefahr einer schleichenden Aushöhlung der Selbstbestimmung, insbesondere durch eine notwendige Einschränkung der Möglichkeiten und die kontextuelle Veränderung der Ausübung der Selbstbestimmung. Die Ergebnisse der Neurodatenverarbeitung können das künftige Verhalten der betroffenen Person intensiv beeinflussen. Zudem wird eine Positionierung des Betroffenen einer Gehirn-Computer-Schnittstelle zu den fortlaufend stattfindenden Informationsprozessen und ihren Ergebnissen insgesamt erschwert, wenn unklar ist, welche Teile der Wahrnehmung auf die eigene Gehirnaktivität zurückgehen und welche Teile die Folge einer hirnstimulierenden Verarbeitung durch einen Algorithmus sind (Kellmeyer, 2021: 91). Die Verarbeitung von Neurodaten könnte sich damit letztlich auf die Beziehung der Person zu sich selbst auswirken (Aufhebung der Ich-Autorität; Gertler, 2020).

3 Vgl. Rainey et al. (2020: 11 ff.) im Anwendungsbereich der DS-GVO.

Hieran knüpft zusätzlich die Frage an, wie dem Problem einer möglichen Diskriminierung durch die Verarbeitung von Neurodaten – ggfs. auch auf legislativer Ebene – begegnet werden kann (Ienca/Ignatiadis, 2020).

Informationelle Unsicherheiten könnten zusätzlich zu technischen Fehlern bei Geräten ursächlich werden für physische Verletzungen, indem etwa bei digital ansteuerbaren Prothesen (oder anderen Hilfsmitteln) aus robustem Material die falschen Steuerungsbefehle ankommen oder eine Fehlerkorrektur der Steuerung erst zeitlich verzögert erfolgt und dadurch der Körper des Patienten selbst oder Menschen in seiner Nähe zu Schaden kommen (Yuste et al., 2017: 159). Die vorgegebenen Einschränkungen verstärken möglicherweise die Risiken für die Selbstbestimmung sowie für eine vorurteilsfreie Entwicklung, Entfaltung und Ausübung von individuellen Anlagen (Kellmeyer, 2021: 91). Dies kann sich auch auf die Art und Weise der Kommunikation und Interaktion mit anderen Personen auswirken. Eine weitere Herausforderung besteht somit darin, dass der Betroffene nicht bloß Input bzw. Vorschläge anhand seiner eigenen bereits getroffenen Entscheidungen erhält, sondern der Algorithmus die verschiedenen Einflüsse und vielfältigen Eindrücke der realen Welt versucht nachzubilden.

16.2 Die Verarbeitung von Neurodaten

16.2.1 Rechtsgrundlage für die Verarbeitung

Vor diesem Hintergrund ist zu überlegen, wie den Aufklärungspflichten im Rahmen einer informierten Einwilligung angemessen Rechnung getragen werden kann. Um ein hinreichendes Verständnis von den angewendeten Technologien zu erlangen und den Betroffenen zu erlauben, die Tragweite der Einwilligung für die anvisierten Verarbeitungskontexte einschätzen zu können, sind umfassende Informationen erforderlich. An die Herausforderung eines erhöhten Kommunikations- und Erklärungsbedarfs schließen zwei Fragen an. Erstens, welche Form der Einwilligung die entsprechende Legitimationsgrundlage bietet, und zweitens, wie mit der Prädiktion und weiteren, neuen Informationen während des Verarbeitungsprozesses umzugehen ist.

Die Verarbeitung sensibler Daten erfordert eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a) DS-GVO). Diese Ausdrücklichkeit wird bei der Verarbeitung von Neurodaten grundsätzlich schwierig zu erreichen sein, denn die hierfür notwendigen Informationen werden bei Erhebung der Daten regelmäßig gerade noch nicht vorliegen und deshalb dem Datensubjekt nicht vermittelt werden können. Die Situation wird erschwert, wenn die Daten für wissenschaftliche Forschungszwecke weiterverarbeitet werden und die Ergebnisse der Analyse ihrerseits erst die weiteren Forschungszwecke

der Daten vorgeben, gegebenenfalls mit einem gewissen zeitlichen Abstand. Im wissenschaftlichen Kontext wird sich die sogenannte breite Einwilligung[4] (Broad Consent) aus demselben Grund als Rechtfertigungsgrundlage für die Verarbeitung dieser Daten wenig eignen. Noch ist nicht abzusehen, wie sich dieses konzeptionelle Problem auf die Diskussion um Broad Consent auswirken wird. Die Datenschutzkonferenz der Aufsichtsbehörden schreibt vor, dass auch eine breite Einwilligung so spezifisch wie nur möglich sein muss.[5] Nach Art. 5 Abs. 1 lit. b) DS-GVO müssen personenbezogene Daten für festgelegte und eindeutige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Es gibt eine („widerlegbare"; Schantz/Wolff, 2017: 135) Vermutung, dass die Verarbeitung zu Forschungszwecken mit anderen Zwecken vereinbar ist (Erwgr. 50 DS-GVO). Die Geeignetheit von Broad Consent hingegen wird danach zu beurteilen sein, welche Zweckbestimmung und Zweckbindung genau zu verlangen ist. Des Weiteren ist zu beachten, dass unter „Forschung" auch die angewandte Forschung verstanden wird (siehe Erwgr. 159 DS-GVO). Sofern die neuen, sekundären Forschungszwecke also nicht de facto unvereinbar mit dem ursprünglichen Zweck sind, sollte die weitere Verarbeitung der Daten zu diesen Zwecken entsprechend erfolgen können.

Die mit der Pflicht des Verantwortlichen zur transparenten Aufklärung einhergehende Schwierigkeit hinsichtlich der Frage, ob trotz unzureichender Informationslage eine *ausdrückliche* Einwilligung erfolgen kann und damit eine taugliche Rechtsgrundlage für die Verarbeitung existiert, setzt sich in allen weiteren Verarbeitungsschritten fort; denn auch hier sind die Informationspflichten nach Art. 13 und 14 DS-GVO zu erfüllen. In der Regel wurden Daten, die weiterverarbeitet werden, ursprünglich direkt bei der betroffenen Person erhoben. Gemäß Art. 13 DS-GVO müssen diese Personen über die Sekundärverarbeitung informiert werden. Hier wurden auf der legislativen Ebene der DS-GVO weder der Unmöglichkeit noch der Verhältnismäßigkeit des Aufwands Rechnung getragen. Die Anforderungen an die Informationspflicht nach Art. 13 DS-GVO sind von den Informationen zu unterscheiden, die im Rahmen der Aufklärung vor einer Einwilligung gegeben werden, andernfalls wäre de facto die Einwilligung die einzige verfügbare Rechtsgrundlage. Demnach besteht die Möglichkeit, die Anforde-

4 Als breite Einwilligung bezeichnet man im Gegensatz zu einer informierten oder spezifischen Einwilligung eine Zustimmung, die nicht nur für einen genau definierten und zum Zeitpunkt der Zustimmung bereits bekannten Sachverhalt gilt, sondern unspezifisch auch für weitere, oft erst im späteren Verlauf einer Studie oder Anwendung erkennbare Nutzungsmöglichkeiten der Daten gültig ist.

5 Datenschutzkonferenz (3. April 2019). Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO.

rungen von Art. 13 DS-GVO auch durch öffentliche Bekanntmachungen oder durch die Bereitstellung von Informationen auf Forschungswebseiten zu erfüllen, wobei die betroffenen Personen stets ausreichend informiert werden müssen, um ihre individuell-subjektiven Datenschutzrechte in Anspruch nehmen zu können.

Ob die Transparenz- und Informationspflichten, die während der Verarbeitung unabhängig von der Rechtsgrundlage oder der Weiterverarbeitung der Daten greifen, doch besser schrittweise und dynamisch zu erfüllen sind, bleibt ebenfalls zu beantworten. Ebenso bedarf es weiterer Überlegung, ob eine Lösung eher in neuen Einwilligungsformen zu suchen ist, etwa der dynamischen Einwilligung (Budin-Ljøsne et al., 2015: 4; Kaye et al., 2015),[6] oder die Verarbeitung von Neurodaten auf andere Rechtsgrundlagen zu stützen ist. Auch bei einer direkten Erhebung der Daten bei dem Betroffenen kann eine andere Rechtsgrundlage für die Verarbeitung transparenter und fairer sein. Zudem bleibt zu berücksichtigen, dass viele andere Rechtsgrundlagen des Art. 9 Abs. 2 DS-GVO bereits im Rahmen der Rechtfertigung die Beachtung von technischen und organisatorischen Maßnahmen vorschreiben. Zwar sind im Rahmen der Sicherheit der Daten nach Art. 25 und Art. 32 DS-GVO solche Maßnahmen unabhängig von der Rechtsgrundlage zu ergreifen. Wenn allerdings Datensicherheitsmaßnahmen als Ergebnis der Abwägung zwischen den Datenschutzinteressen der Betroffenen und den Verarbeitungsinteressen in die tatbestandliche Ausgestaltung der Rechtsgrundlage einbezogen werden, sind diese bereits Teil der Legitimation der Datenverarbeitung. Ihnen kommt dadurch eine herausgehobene Stellung zu. Eine solche Stellung ist angemessen, wenn der Betroffene in seinen rechtlichen Möglichkeiten, die Verarbeitung der Daten mitzubestimmen, eingeschränkt ist.

16.2.2 Datenschutzrechte der Betroffenen

Die individuellen Datenschutzrechte der Betroffenen gestalten das Grundrecht auf Datenschutz näher aus. Sie erlauben den Betroffenen ein Maß an Kontrolle in den verschiedenen Phasen der Datenverarbeitung. Grundlage für diese Kontrolle sind die umfassenden Informationspflichten, die in Art. 13 und 14 DS-GVO definiert sind.

Durch die speziellen Eigenschaften von Neurodaten und die Besonderheiten ihrer Verarbeitung (siehe 16.1) sind die Kontrollmöglichkeiten der Betroffenen eher eingeschränkt. Um die individuell-subjektiven Rechte des Kapitels III DS-GVO in Anspruch zu nehmen, sind nicht nur umfassende Informationen über die Verarbeitung notwen-

6 Die dynamische Einwilligung sieht eine kontinuierliche Information und jeweils erneute Einholung der Zustimmung für weitere, in der ursprünglichen Aufklärung noch nicht absehbare Datennutzungen vor.

dig; zusätzlich ist zu gewährleisten, dass der Betroffene sich zu der Verarbeitung unmittelbar und bewusst verhalten kann. Dies ist bei vielen Verarbeitungsvorgängen von Neurodaten wegen ihrer unmittelbaren Verbindung zum kognitiven System des Betroffenen ohne zusätzliche Informationen nicht gegeben.

Ersichtlich ist die Einschränkung vor allem bei der Anwendung des Rechts auf Vergessenwerden, das das permanente Fortbestehen von Informationen über eine Person verhindern soll und damit der Möglichkeit einer freien Entfaltung der Persönlichkeit dient. Der Begriff des Vergessens schließt nicht notwendigerweise einen Dritten ein, sondern meint das Verschwinden der Information als solche (Molnár-Gábor, 2019: 98 ff.). Bezogen auf Neurodaten gewinnt das Recht auf das eigene Vergessen der Daten zunehmend an Bedeutung. Wegen der unmittelbaren Nähe dieser Daten zur betroffenen Person und ihrer Identität wird es zunehmend schwierig zu unterscheiden, welches Datum einerseits als Grundlage für Entscheidungsfindungen ohne Mitwirkung von BCI-Technologien diente und welches Datum andererseits in irgendeiner Form an die betroffene Person doch zurückgegeben und damit in die Struktur ihrer Entscheidungsfindung einbezogen wurde. Das eigene Vergessen ist notwendig, wenn sich die Informationsverarbeitung von der betroffenen Person löst und verselbstständigt, um dann wieder in ihre eigenen Entscheidungsprozesse eingespeist zu werden.

16.2.3 Anonymisierung

Anonymisierte Daten sind nicht personenbezogen und unterfallen damit nicht dem Anwendungsbereich der DS-GVO. Zunehmend setzt sich ein relatives Verständnis der Datenanonymität durch, wonach über die Klassifizierung der Daten als personenbezogen nur anhand des konkreten Datenverarbeitungsvorgangs und des Verantwortlichen entschieden werden kann.[7] Der Personenbezug entscheidet sich demnach nicht nach theoretischen Möglichkeiten einer Verknüpfung, sondern danach, ob nach den dem Verantwortlichen zur Verfügung stehenden Mitteln und dem Zusatzwissen, auf das er vernünftigerweise Zugriff hat, der Bezug tatsächlich hergestellt werden könnte. Der Schritt der Anonymisierung selbst ist weiterhin als Datenverarbeitung anzusehen (Art. 4 Nr. 2 DS-GVO) und muss auf eine Rechtsgrundlage, ggf. die ausdrückliche Einwilligung des Betroffenen, gestützt werden. Dies könnte sich bei Neurodaten als schwierig erweisen (siehe oben). Die Daten können pseudonymisiert werden, sodass zusätzliche Zuordnungsregeln herangezogen werden müssen, um die Datensätze mit der betroffenen Person zusammenzuführen. Solche Daten fallen in den Anwendungsbereich der

7 EuGH, C-582/14 – Breyer, Rn. 42 ff.

DS-GVO gem. Art. 4 Nr. 5. Pseudonymisierte Daten, die bei einem anderen Verantwortlichen ankommen als dem, der die Verschlüsselung durchgeführt hat, können als anonyme Daten behandelt werden, wenn der neue für die Verarbeitung Verantwortliche nicht über rechtliche oder praktikable Mittel verfügt, das Pseudonym in die Identität der betroffenen Person umzukehren.

Das Cross-Referencing von Neurodaten mit anderen Daten ermöglicht ggf. die Aufhebung der Pseudonymisierung der Daten (Kellmeyer, 2021: 87). Wer letztendlich welchen Zugriff auf welche Daten mit welcher Technologie hat, ist womöglich die entscheidende Frage, die eine große praktische Bedeutung für die Anwendung des Datenschutzrechts bei der Verarbeitung von Neurodaten haben wird. Hervorzuheben ist dabei, dass der Schritt der Weitergabe oder Veröffentlichung von pseudonymisierten Daten durch den ursprünglichen Verarbeiter, der den Zuordnungsschlüssel hat, als eine Verarbeitung personenbezogener Daten zu klassifizieren ist. Dieser Verarbeitungsschritt muss den datenschutzrechtlichen Anforderungen ebenso genügen, insbesondere hat er in einer für die betroffene Person nachvollziehbaren Weise zu erfolgen (sog. Transparenzprinzip, Art. 5 Abs. 1 lit. a DS-GVO). Betroffene Personen können ihre Rechte nach der DS-GVO gegenüber dem ursprünglichen Verarbeiter weiterhin geltend machen. Womöglich muss der Verantwortliche, bevor Daten anonymisiert weitergegeben werden, eine Risikoeinschätzung (ähnlich der Datenschutz-Folgenabschätzung) durchführen, um zu erschließen, ob vernünftigerweise bestehende Optionen einer Identifizierung ausgeschlossen werden können.

Dies bedeutet gleichwohl, dass mit anonymisierten Daten nicht beliebig verfahren werden darf; dies gilt vor allem, wenn ihre Vernetzung sie besonders anfällig für die Aufhebung ihrer Anonymität in Bezug auf die betroffene Person macht. Besondere Aufmerksamkeit verdienen Sachverhalte, in denen Neurodaten zunächst nicht in den Anwendungsbereich des Datenschutzrechts fallen, deren De-Anonymisierung aber später durch weitere Verknüpfungen stattfinden könnte. Diese Herausforderung gilt allgemein, kommt aber wegen des hohen Individualisierungsgrads von Neurodaten („brain fingerprinting"; Kumar et al., 2018) – ähnlich wie bei genomischen Daten – stärker zum Tragen.

16.3 Datenschutz als Teil der Regelungslösung

Neurodaten werden nicht um ihrer selbst willen geschützt, sondern wegen ihrer umfassenden Aussagekraft über das kognitive System des Menschen. Mithilfe von Neurotechnik kann das kognitive System auf die Umwelt ausgedehnt werden („extended mind"; Blitz, 2010: 1049). Deshalb müssen die Grenzen des schutzwürdigen kognitiven Systems

definiert und der befugte Zugriff darauf bestimmt werden. Ein wesentliches Element des Zugriffs auf das kognitive System des Menschen erfolgt über die Verarbeitung von Neurodaten. Das Datenschutzrecht kann einen Eckpfeiler eines Schutzes darstellen.

Zu den datenschutzrechtlichen Lösungen, die zur Wahrung der relativen Anonymität beitragen, zählen Maßnahmen wie die lokale Speicherung von Daten, Übermittlungsverbote und die nicht zentralisierte, sondern verteilte (föderierte) Auswertung der Daten. Des Weiteren ist die Einführung spezifischer Einwilligungsregeln sowie das Etablieren von Transparenzpflichten entscheidend, um die Inanspruchnahme der Betroffenenrechte zu ermöglichen. Technische Entwicklungen für die Verarbeitung von Neurodaten, die über eingebettete Datenschutzeinstellungen verfügen, können ergänzend für die vereinfachte Einhaltung spezifischer Datenverarbeitungsvorschriften sorgen.

Die Dringlichkeit, das Thema Datenschutz kontextbezogen zu begreifen, wird am Beispiel von Neurodaten ersichtlich. Instrumente, die im Einklang mit geltenden datenschutzrechtlichen Regelungen stehen und sektorspezifische Bestimmungen definieren, können zu Verbindlichkeit und Akzeptanz beitragen. Die DS-GVO zeigt beispielhaft die Möglichkeit von Verhaltenskodizes auf (Art. 40). Solche Instrumente können von Akteuren, die einem bestimmten Datenverarbeitungsbereich zuzuordnen sind, etabliert oder unterstützt werden. Auf diese Weise wird durch die Einbindung der sektorspezifischen Kenntnis eine wertvolle Perspektive hinzugefügt und die Vornahme der Datenschutz-Folgenabschätzung in einem bestimmten Verarbeitungsbereich verbessert und vereinfacht. Dies ermöglicht den Betroffenen eine Beurteilung der Risiken und erleichtert den Nachweis über die Einhaltung der datenschutzrechtlichen Vorgaben.

Indem die kontextbezogenen Verarbeitungsregeln den Datenschutz stets in Relation zum typisierten Verarbeitungsvorgang definieren, können sie dazu beitragen, auch die Übergänge zwischen datenschutzrechtlich relevanten und irrelevanten Verarbeitungen für den Umgang mit Neurodaten zu definieren. Dies legt nahe, dass der datenschutzkonforme Umgang mit Daten, die von spezifischem Schutzbedarf sind, auch eine erhebliche organisatorische Aufgabe darstellt. Zielführend erscheint die Erstellung eines umfassenden Konzepts im Sinne einer Informations-Governance (siehe auch Winkler/Prainsack, Kap. 17).

Allgemein ist festzuhalten, dass sich im medizinischen Bereich das Einbeziehen von außerrechtlichen Normen in Form der Medizinethik erfolgreich etabliert hat und als interdisziplinäres Forum der Verständigung Anerkennung findet. Hierdurch kann über die rein rechtliche Situation *de lege lata* hinaus zu einer Regelungslösung beigetragen werden, die den Herausforderungen umfassend Rechnung trägt. Es ist wünschenswert, dass sich diese Entwicklung auf dem rechtlich und technologisch vergleichsweise jun-

gen Gebiet der Neurodatenverarbeitung fortsetzt. Die aktuellen Weichenstellungen bereiten idealerweise einen Rahmen vor, in dem Gehirn-Computer-Schnittstellen durch ihr bedeutendes Potenzial die physischen Umstände von Personen verbessern und gleichzeitig ihre mentale und private Integrität erhalten.

16.4 Literaturverzeichnis

Blitz, M. J. (2010): Freedom of thought for the extended mind: cognitive enhancement and the constitution. In: Wisconsin Law Review 4.

Budin-Ljøsne, I. et al. (2017): Dynamic consent: a potential solution to some of the challenges of modern biomedical research. In: BMC Med Ethics 18(1): 4.

Chaudhary, U. et al. (2016): Brain-computer interfaces for communication and rehabilitation. In: Nat Rev Neurol. 12(9): 513–525.

Chaudhary, U. et al. (2017): Erratum. In: Nat Rev Neurol. 13(3): 191.

Gertler, B. (2020): Self-Knowledge. In: Zalte, E. N. (Hrsg.): The Stanford Encyclopedia of Philosophy, 1.4. Unter: https://plato.stanford.edu/archives/spr2020/entries/self-knowledge [06.06.2021].

Hermstrüwer, Y. (2016): Informationelle Selbstgefährdung. Mohr Siebeck, Tübingen.

Ienca, M./Ignatiadis, K. (2020): Artificial intelligence in clinical neuroscience: Methodological and ethical challenges. In: AJOB Neurosci. 11(2): 77–87.

Kaye, J. et al. (2015): Dynamic consent: a patient interface for twenty-first century research networks. In: Eur J Hum Genet 23: 141–146.

Kellmeyer, P. (2021): Big brain data: On the responsible use of brain data from clinical and consumer-directed neurotechnological devices. In: Neuroethics 14: 83–98.

Kinney-Lang, E. et al. (2020): Designing a flexible tool for rapid implementation of brain-computer interfaces (BCI) in game development. In: Annu Int Conf IEEE Eng Med Biol Soc.: 6078–6081.

Kumar, K. et al. (2018): Multi-modal brain fingerprinting: A manifold approximation-based framework. In: Neurolmage 183: 212–226.

Lavazza, A. (2018): Freedom of thought and mental integrity: The moral requirements for any neural prothesis. In: Front Neurosci. 12(82).

Leeb, R./Pérez-Marcos, D. (2020): Brain-computer interfaces and virtual reality for neurorehabilitation. In: Handb Clin Neurol. 168: 183–197.

Milekovic, T. et al. (2018): Stable long-term BCI-enabled communication in ALS and locked-in syndrome using LFP signals. In: J Neurophysiol. 120(1): 343–360.

Molnár-Gábor, F. (2019): Das Recht auf Nichtwissen – Fragen einer Verrechtlichung im Kontext von Big Data in der modernen Biomedizin. In: Duttge, G./Lenk, C. (Hrsg.): Das sogenannte Recht auf

Nichtwissen: Normatives Fundament und anwendungspraktische Geltungskraft. Mentis, Paderborn: 83–117.

Moos, T. et al. (Hrsg.) (2011): Genetisches Wissen. Röhrig Universitätsverlag, St. Ingbert.

OECD (2020): Recommendation of the Council on Responsible Innovation in Neurotechnology, II. Unter: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457 [06.06.2021].

Purtova, N. (2018): The law of everything. Broad concept of personal data and future of EU data protection law. In: Law, Innovation and Technology 10(1): 40–81.

Rainey, S. et al. (2020): Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology? In: Journal of Law and the Biosciences 7(1).

Schantz, P./Wolff, H. A. (2017): Das neue Datenschutzrecht. C. H. Beck, München.

Taylor, M. (2012): Genetic data and the law: A critical perspective on privacy protection. Cambridge University Press, Cambridge.

Wang, Y. et al. (2019): EEG-based brain-computer interfaces. In: Adv Exp Med Biol. 1101: 41–65.

Yuste, R. et al. (2017): Four ethical priorities for neurotechnologies and AI. In: Nature 551(7679): 159–163.