Stellungnahme Nr. 28 der Europäischen Gruppe für Ethik in Naturwissenschaften und Neuen Technologien bei der Europäischen Kommission

20 Mai 2014

Ethik der Sicherheits- und Überwachungstechnologien

Brüssel, 20 Mai 2014

Bezug: Ersuchen von Präsident Barroso

Berichterstatter: Inez de Beaufort, Linda Nielsen, Siobhán O'Sullivan

Nur der Originaltext auf Englisch ist authentisch.

Empfehlungen

Eine Stellungnahme zu ethischen Implikationen von Sicherheits- und Überwachungstechnologien zu formulieren, wie die EGE gebeten wurde zu verfassen, stellt eine dringliche, aber schwierige Aufgabe. Denn die genannten Technologien haben sehr unterschiedliche Zwecke, werden von unterschiedlichen Akteuren verwendet, bringen verschiedene Stufen und Formen von Gefährdungen der Menschenrechte mit sich und führen zu unterschiedlichen Nutzungsformen.

Die zunehmende Verfügbarkeit von grossen Informationsmengen und die steigende Anzahl von Kommunikationsnetzen sind wichtige Faktoren, die die Globalisierung des 20. Jahrhunderts mit sich gebracht hat. Als weitere Merkmale einer globalisierten Welt lassen sich das Unsicherheitsgefühl, mangelndes Vertrauen und eine geringe Risikotoleranz benennen. Schiessereien in Schulen, Kinos und Einkaufszentren, Sprengstoffanschläge in U-Bahnen, Zügen und im Luftverkehr, Kindesentführungen, Prügelattacken und Raubüberfalle auf ältere Menschen haben dazu beigetragen, dass unser Unsicherheitsgefühl auch in unserem eigenen Umfeld stärker geworden ist. Auch wenn alle objektiven Beurteilungen zeigen, dass es nie eine Zeit gab, in der das Leben sicherer war als heute, bleibt dieses Unsicherheitsgefühl bestehen. Der Wunsch der Regierungen, auf dieses von den Bürgern wahrgenommene Unsicherheitsgefühl zu reagieren, hat zweifellos zu einer Ausweitung sicherheitspolitischer Massnahmen in Europa und anderswo geführt.

Sicherheit, im eher engen Wortsinn verwendet, beinhaltet den Schutz vor körperlichen Schäden oder der Androhung von Schaden und ist ein wesentlicher Bestandteil des Wohlbefindens. Im Sinne eines Gesellschaftsvertrages verstanden, haben sich Staaten verpflichtet, im Austausch für das Zugeständnis, die Freiheit des Einzelnen zu beschneiden, für die Sicherheit der Bürger zu sorgen. Dies ist jedoch nur ein Aspekt des Sicherheitsparadigmas. Der Schutz der körperlichen Unversehrtheit ist notwendig, aber nicht ausreichend. Sicherheit muss in einem breiteren Kontext betrachtet werden, der sowohl menschliche als auch gesellschaftliche Sicherheit umfasst. Dies erfordert, dass wir unsere Überlegungen zum Sicherheitsverständnis

von der Bedeutung des Staates zu der von Einzelpersonen, Gesellschaftsgruppen und Wirtschaftsunternehmen erweitern. Europa ist eine Wertegemeinschaft, in der wir uns bemühen, Würde, Autonomie, Freiheit und Gerechtigkeit durch Menschenrechte zu schützen. Diese Werte und Güter schaffen ein Umfeld, in dem sich der Einzelne durch Kreativität, Innovation, Entwicklung von starken persönlichen Beziehungen zu anderen und durch den dadurch möglichen Beitrag zur Gesellschaft entfalten kann. Bildung, Gesundheit, Demokratie, Umwelt und Gleichheit sind wesentliche Bausteine eines sicheren Europas.

Ein eher begrenzter Ansatz zur Verwirklichung von Sicherheit, ganz besonders, wenn es um die enge Auslegung dieses Begriffs als Staatssicherheit geht, besteht darin, Kompromisse zu schliessen. Das klassische Beispiel dafür ist der Kompromiss zwischen Freiheit, oft als Datenschutz bzw. Privatsphäre bezeichnet, und Sicherheit. Eine ausgewogene Balance zwischen konkurrierenden Prinzipien oder Werten muss hergestellt werden, wenn diese in Konflikt geraten. Es gibt aber einige Grundprinzipien wie die Menschenwürde, die in keinem Fall geopfert werden dürfen. Dies erfordert, dass wir über die Rhetorik von Kompromissen hinausgehen und eine differenziertere Vorgehensweise anstreben, bei der Sicherheitstechnologien und Massnahmen auf der Grundlage der Verhältnismässigkeit und Wirksamkeit geprüft und Rechte priorisiert und nicht geopfert werden.

Die EGE erkennt an, dass die Staatsgewalt in einer demokratischen Gesellschaft in völlig legitimer Weise Behörden und Einrichtungen dazu einsetzt, nach strengen gesetzlichen Vorschriften die Überwachung als Mittel zur Wahrung der Sicherheit ihrer Bürger zu nutzen. Die EGE vertritt auch die Auffassung, dass Geheimhaltung und Diskretion ein wesentlicher Teil der Würde des menschlichen Lebens sind. Die Verletzung des Rechts einer Person auf Privatsphäre durch eine Behörde muss begründet werden und gerichtlicher Aufsicht unterliegen. Die Überwachung muss notwendig und verhältnismässig sein, um eine entsprechende Relation zwischen den ergriffenen Massnahmen und den erreichten Zielen zu gewährleisten. Ein entscheidendes Kriterium für die Beurteilung der Verhältnismässigkeit ist die Wirksamkeit des jeweiligen Eingriffs. Diese Wirksamkeit muss regelmässig überprüft werden. Die Befugnis zur Überwachung muss für einen bestimmten Zweck und für einen bestimmten Zeitraum gewährt werden. Alternativen, die das gleiche Ziel erreichen können, müssen geprüft und dokumentiert werden, um die am wenigsten eingriffstiefe Methode zu wählen. Rechenschaftspflicht ist eine notwendige Voraussetzung für die öffentliche Überwachung. Folglich muss die Überwachung evidenterweise aus angemessenen Gründen und in Übereinstimmung mit öffentlich zugänglichen Verfahrensregeln erfolgen. Sicherheits- und Überwachungstechnologien müssen so transparent wie möglich angewendet werden, wobei legitime Ausnahmen ausdrücklich im Rechtssystem bestimmt werden. An der Überwachung beteiligte private oder gewerbliche Organisationen sind ebenfalls an die oben genannten Kriterien gebunden.

Vor diesem Hintergrund gibt die drohende Diskriminierungsgefahr Grund zur Sorge. Denn wir müssen uns über die möglichen unerwarteten Auswirkungen der allgegenwärtigen Überwachung bewusst sein. Sie zwingt den Einzelnen dazu, sich mit entsprechenden Formen der Normalität (verstanden als implizite Normativität) abzufinden, sich folglich anders zu verhalten und diese Norm weiter zu verstärken, was wiederum zu einer verarmten - wenn nicht sogar steril gemachten - Gesellschaft führt (in der Vielfalt, Kreativität und sogar Zusammenhalt ausgemerzt wurden). Die Diskriminierung kann abzielen auf die Überwachung bestimmter Minderheiten, und die EGE fordert Abhilfemassnahmen, wenn es in den EU-Mitgliedstaaten zu solchen Fällen kommt. Weiterhin kann Diskriminierung Profiling und Stigmatisierung betreffen. Es muss anerkannt werden, dass Profiling vielfältige Formen annehmen kann, von Programmen, bei denen man sich selbst für die Teilnahme entscheiden kann (wie das Global-Entry-Programm), bis hin zu „Facecrime“ und Gesichtserkennung (sowie anderen

biometrischen Systemen) und zur Erstellung von Persönlichkeitsprofilen aller Bürger durch Massenüberwachung. Stigmatisierung (und ihre Entsprechung, die Demütigung) müssen selbstverständlich vermieden werden, doch die Rolle, die die zunehmend allgemeine Verwendung der Algorithmen als Teil der Ansammlung von Sicherheits- und Überwachungsdaten spielt, ist in dieser Hinsicht besonders alarmierend. Diese Algorithmen können die ethische Reflexion und Rechtfertigung von Entscheidungen verschleiern oder für sich einnehmen, was zu „In-built-Profiling “oder „Stigmatisierung by Design“ führt. Dabei riskiert man auch die Perfektionierung der Normalität und Compliance, auf die oben hingewiesen wurde, durch unübersichtliche Auswahlprozesse, damit menschliches Eingreifen und Verstehen ferngehalten wird. Die EGE ist sich in dieser Hinsicht der Gefahr der Instrumentalisierung von Ethikräten und verwandten Einrichtungen bei diesen Prozessen der Normalisierung in Bezug auf neue Technologien vollständig bewusst. Ebenfalls ist sich die EGE der Schwierigkeiten in Gänze bewusst, die darin liegen, die Sicherheits- und Überwachungstechnologien aus ethischer Sicht zu betrachten, ohne dass dies als eine Form des stillschweigenden Duldens verstanden wird. Die EGE ist entschlossen, diese Schwierigkeiten nicht zu scheuen, sondern sie in dieser Stellungnahme direkt anzugehen.

Basierend auf den skizzierten Überlegungen, ist die EGE in den folgenden Empfehlungen auf dem Gebiet der Sicherheits- und Überwachungstechnologien übereingekommen:

I. Technologien, die möglicherweise die Privatsphäre von Personen verletzen könnten, die ihrerseits nicht die Möglichkeit haben, ihr Einverständnis zu erklären (oder die ihre Ablehnung nicht kundtun können), erfordern eine spezifische Rechtfertigung. Die EGE fordert jeweils Begründungen für jeden Einzelfall dieser Massnahmen.

1. Rechenschaftspflicht

Die Mitgliedstaaten müssen sicherstellen, dass Personen oder Einrichtungen, die berechtigt sind, die Privatsphäre der Bürger zu überwachen, im öffentlichen Interesse handeln und Rechenschaft über ihr Handeln ablegen. Wenn der Staat Sicherheits- und/oder Überwachungsaufgaben an private Unternehmen delegiert, sind diese an die gleichen rechtlichen und ethischen Verpflichtungsstandards gebunden. Die Mitgliedstaaten müssen gewährleisten, dass die Einhaltung dieser Verpflichtungen überwacht wird.

2. Gerichtliche Kontrolle

Die Mitgliedstaaten müssen über ein System der gerichtlichen Kontrolle von behördlichen Überwachungsmassnahmen bei strafrechtlichen Ermittlungen verfügen. Der Einzelne muss nachträglich informiert werden, dass er überwacht wurde, vorausgesetzt, dass dadurch die Ermittlung nicht beeinträchtigt wird. Der Einzelne muss die Möglichkeit haben, auf dem Gerichtsweg Entschädigung zu beantragen, wenn er Objekt einer rechtswidrigen Überwachung wurde.

3. Entwicklung eines gemeinsamen Verständnisses von nationaler Sicherheit

Die in der Charta der Grundrechte verankerten gemeinsamen europäischen Werte stellen den normativen Rahmen dar, auf dem ein gemeinsames ethisches Verständnis von nationaler Sicherheit aufgebaut werden kann.

a) Es wird anerkannt, dass nationale Sicherheit legitim im Zentrum der jeweiligen nationalen Interessen steht und in die Zuständigkeit der Mitgliedstaaten fällt. Die EGE empfiehlt jedoch, dass die EU-Organe in Zusammenarbeit mit den Mitgliedstaaten auf ein gemeinsames

Verständnis nationaler Sicherheit hinwirken.

b) Die EGE empfiehlt auch, dass die Mitgliedstaaten Verfahren etablieren, um andere Mitgliedstaaten entsprechend über nachrichtendienstliche Tätigkeiten ausserhalb ihres Hoheitsgebiets zu informieren, um das Vertrauen zwischen den Partnern zu bewahren.

c) Die Mitgliedstaaten dürfen nicht im Namen der nationalen Sicherheit andere Mitgliedstaaten überwachen, um kommerzielle Vorteile zu erzielen, weil ein solches Verhalten im Widerspruch zum Ziel der EU steht, einen einheitlichen europäischen Markt zu schaffen.

4. Drohnen

Die rasante Entwicklung und der vermehrte Einsatz von Drohnen in militärischen, zivilen und wirtschaftlichen Zusammenhängen durch die Mitgliedstaaten wurden nicht von den notwendigen Entscheidungsstrukturen und Kontrollregelungen begleitet. Diese sind derzeit bestenfalls fragmentarisch. Der EU fehlt ein umfassender Rechtsrahmen für die Entwicklung, den Erwerb, den Einsatz und den Export von Drohnen für den zivilen und wirtschaftlichen Einsatz. Die EGE begrüsst die bereits von der Europäischen Kommission getroffenen Massnahmen hinsichtlich der Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in das EU-Luftverkehrssystem (einschliesslich umfassende Konsultation und Veröffentlichung eines Fahrplans). Es verdient Anerkennung, dass dabei von Anfang an die Betrachtung der gesellschaftlichen Auswirkungen des Drohneneinsatzes einbezogen wurden.

a) Angesichts des jüngsten Engagements der EU für eine verbesserte Koordinierung zwischen den Mitgliedstaaten bei der Entwicklung und Beschaffung von Drohnen empfiehlt die EGE, dass diese Zusammenarbeit auf die Erarbeitung gemeinsamer Normen und rechtlicher Rahmenbedingungen für die zivile und kommerzielle Nutzung von Drohnen in der EU ausgedehnt wird. Besonderes Augenmerk muss auf eine Bewertung der bestehenden EU-Datenschutzregelungen gerichtet werden, um beurteilen zu können, ob die derzeitigen Rechtsvorschriften im Hinblick auf die Integration ferngesteuerter Luftfahrzeuge (Remotely Piloted Aircraft Systems, RPAS) in den europäischen Luftraum ihren Zweck erfüllen.

b) Die Mitgliedstaaten müssen dafür sorgen, dass die nationale Politik in Bezug auf den Einsatz von Drohnen im Inland (d.h. innerhalb der jeweiligen nationalen Grenzen), im öffentlichen Raum, nicht die Menschenrechte der Personen verletzen, die von den Drohneneinsätzen betroffen sind. Die Nutzung von Drohnen auf dem eigenen Staatsgebiet muss einer Zulassung und geeigneten Aufsicht unterliegen, um die Sicherheit zu gewährleisten und Missbrauch zu verhindern. Ausserdem müssen Personen, die Genehmigungen für den Einsatz von Aufklärungsdrohnen beantragen, nachweisen, dass die beabsichtigte Nutzung gerechtfertigt, notwendig und verhältnismässig ist. Die EGE empfiehlt auch, dass die Reglungen und Verfahren für den innländischen Einsatz von Drohnen zum Überwachungszwecke im Interesse der Transparenz, die wiederum eine Voraussetzung für das Vertrauen der Öffentlichkeit bildet, öffentlich zugänglich sein müssen.

c) Die EGE lenkt die Aufmerksamkeit auf die gravierenden ethischen Auswirkungen der militärischen Nutzung von Drohnen sowie der automatisierten Kriegsführung und begrüsst die Entschliessung des Europäischen Parlaments zum Einsatz von bewaffneten Drohnen vom 25. Februar 2014. Die EGE fordert mehr Transparenz und Rechenschaftspflicht auf Seiten derjenigen Mitgliedstaaten, die Drohnen für militärische Zwecke einsetzen. Zu diesem Zweck müssen die Mitgliedstaaten die rechtliche Grundlage, den Umfang und Grenzen aller tödlichen Drohnenangriffe offenlegen und es muss eine Untersuchung stattfinden, dass die für

traditionelle bewaffnete Konflikte geltenden rechtlichen Rahmenregeln nicht verletzt werden. Informationen über die Anzahl von Zivilisten und Nicht-Zivilisten, die bei Drohnenangriffen getötet werden, sollten ebenfalls öffentlich zugänglich gemacht werden. Ferner befürwortet die EGE ausdrücklich Untersuchungen, um die ethischen Implikationen der tödlichen Drohnenangriffe und deren Kompatibilität oder anderweitige Aspekte mit der Theorie des gerechten Krieges zu prüfen. Darüber hinaus sind Studien zur Rolle des moralischen Handels erforderlich, wenn Drohnen ferngesteuert betrieben werden. Dasselbe gilt auch für die Entwicklung von Drohnen mit Selbststeuerung.

II. In Bezug auf Überwachungstechnologien muss die Beweislast bei den Staaten und/oder Unternehmen liegen, die öffentlich und transparent Nachweise erbringen müssen, bevor Sie Überwachungsaktionen durchführen,

- dass diese notwendig sind,

- dass diese wirksam sind,

- dass diese verhältnismässig sind (z. B. durch Angabe der Zweckbindung),

- dass es keine besseren Alternativen gibt, die diese Überwachungstechnologien ersetzen könnten.

Die Einhaltung dieser Kriterien ist einer nachträglichen Beurteilung zu unterziehen. Dies muss entweder auf der Ebene der normalen politischen Analysen oder durch die diesbezüglichen Regelungen der Mitgliedstaaten geschehen.

Ausserdem ist zu beachten:

Rechenschaftspflicht bedeutet, dass alle Menschen das Recht haben, über Überwachungstechnologien informiert zu werden – auch wenn diese Information in einigen Fällen erst nachträglich zur Verfügung gestellt wird.

Transparenz über die wirtschaftlichen Interessen muss jederzeit gewährleistet werden.

5. Personenbezogene Daten

Die EGE betont, dass Zweckbindung hinsichtlich der personenbezogenen Daten eine Standardnorm für öffentliche wie private Organisationen zu sein hat. Personenbezogene Daten sollten nur für einen spezifischen und rechtmässigen Zweck gesammelt werden. So weit wie möglich sollten Daten anonymisiert und die Verschlüsselung stärker genutzt werden, um sowohl den Datenschutz als auch die Sicherheit zu erhöhen. Standardmässige Datenfreigabe ist zu vermeiden und Nutzer sollten die Möglichkeit haben (z. B. durch den Zugang zu Datenschutzeinstellungen), Informationen, die Organisationen über sie besitzen, zu kontrollieren und zu berichtigen. Das Profiling von Personen für kommerzielle Zwecke soll der ausdrücklichen Zustimmung der Betroffenen unterliegen. Informationen von kommerziellen Unternehmen sollten im Hinblick darauf zur Verfügung stehen, wofür Daten gesammelt werden, von wem, zu welchem Zweck, wie lange und ob die Daten die gesammelt werden, mit anderen Datenquellen verknüpft werden.

6. Das öffentliche Bewusstsein für Datenrichtlinien

Die EGE bekräftigt ihre Auffassung, dass die Öffentlichkeit besser darüber aufgeklärt werden

muss, wofür, wie, warum und zu welchem Zweck personenbezogene Daten verarbeitet, weitergegeben und geschützt werden. Behörden und Unternehmen müssen ihre Regelungen in diesem Zusammenhang öffentlich zugänglich machen. Die EU und die Mitgliedstaaten sollen sich bemühen, die Öffentlichkeit über die Folgen der Verwendung von Sicherheits-und Überwachungstechnologien für den Einzelnen und die Gesellschaft aufzuklären, das Bewusstsein für diese Problematik zu schärfen und die Debatte zu diesem Thema zu fördern. Aufklärungsprogramme müssen bereits in der Schule beginnen und Informationen und Instrumente für die Bürger bereitstellen, damit diese ihre Daten in der digitalen Umwelt schützen können.

7. Big Data

Die EGE hat festgestellt, dass mehr und mehr dazu übergegangen wird, grosse Datenmengen, sogenannte „Big Data“, zu sammeln und miteinander in Beziehung zu setzen. Während die EGE den potenziellen Wert solcher Datensätze anerkennt, sind wir besorgt, dass ohne angemessene Sorgfalt im Umgang mit diesen Daten der Grundsatz der Zweckbindung als Mittelpunkt des Datenschutzes untergraben wird. So fordert die EGE Behörden und private Organisationen dringend auf, aussagekräftige ethische Untersuchungen anzustellen, um ihr Handeln mit den gemeinsamen europäischen Werten der Würde, Privatsphäre und Autonomie zu durchdringen und in Einklang zu bringen. Die EGE empfiehlt, dass die EU einen Verhaltenskodex für die Big-Data-Analyse entwickelt, der Unternehmen bei diesem Prozess unterstützen würde.

8. Algorithmen

Im Kontext der Sicherheits-und Überwachungstechnik muss beachtet werden, dass Algorithmen in ihrer Konstruktion notwendigerweise selektiv sind und von den Menschen, die sie programmieren, beeinflusst werden können. Algorithmen und ihren Parametern liegen ethische Annahmen zugrunde, die obligatorisch explizit gemacht werden sollten. Ausserdem sind Algorithmen nicht unfehlbar und die generierten Daten hängen von der Auswahl und Qualität der Dateneingabe ab, die nach Ansicht der EGE ständig geprüft und validiert werden sollte. Darüber hinaus sollte die Aufklärung über die ethischen Aspekte bei der Gestaltung von Algorithmen in die Ausbildung von Entwicklern aufgenommen werden.

9. Datenschutz im Bereich der elektronischen Kommunikation (e-Privacy)

Die EGE empfiehlt der Kommission, in Erwägung zu ziehen, die E-Privacy-Richtlinie zu überarbeiten, die derzeit den Rechtsrahmen für den Umgang mit elektronischer Kommunikation darstellt. Angesichts des rapiden Ansteigens der Zahl der digitalen Schnittstellen seit der Einführung der Richtlinie hält es die EGE für angemessen, dass Produkte, die VoIP – Voice over Internet Protocol, IP-Kommunikation oder Breitbandkommunikation – verwenden, und auch private Unternehmensnetze in den Geltungsbereich einer überarbeiteten Richtlinie einbezogen werden.

10. Datenschutz-Folgenabschätzung

Die Mitgliedstaaten müssen in ihre Prüfungs- und Regulierungstätigkeit Verfahren zur Datenschutz-Folgenabschätzung einbeziehen, wenn neue oder geänderte Informationssysteme, die personenbezogene Daten verarbeiten, auf den Markt kommen. Die Bewertung muss die möglichen Auswirkungen der vorgeschlagenen Technologie für personenbezogene Daten berücksichtigen. Werden Risiken ermittelt, müssen Massnahmen ergriffen werden, um Prozesse zur Senkung dieser Risiken zu identifizieren oder Alternativen zu

dem zu finden, was vorgeschlagen wird.

11. Migration und Grenzkontrolle

Grenzkontrollen sind ein Bereich, in dem Sicherheits- und Überwachungstechnologien sehr verbreitet sind. Dies wirft sowohl global als auch in den EU-Mitgliedstaaten einige Bedenken hinsichtlich der Auswirkungen auf die Menschenrechte und das Solidaritätsprinzip auf. Die EGE empfiehlt, die Grenzkontrollsysteme im Hinblick auf die in dieser Stellungnahme aufgestellten Kriterien, nämlich Menschenwürde und Menschenrechte, Gerechtigkeit, Notwendigkeit, Verhältnismässigkeit, Wirksamkeit, Alternativen und Rechenschaftspflicht zu beurteilen.

Im Einklang mit den Ergebnissen der Artikel-29-Arbeitsgruppe ist die EGE besorgt, dass das Einreise-/Ausreisesystem (Entry-Exit-System – EES), das im Rahmen der Grenzinitiative „Smart Borders“ vorgeschlagen wird, einen unverhältnismässigen Eingriff in die individuelle Privatsphäre darstellt. Laut dem Stockholmer Programm sollten neue Systeme nur dann entwickelt werden, wenn festgestellt wird, dass die bestehenden Systeme nicht ausreichen. Die EGE ist nicht davon überzeugt, dass dieses Kriterium beim Einreise-/Ausreisesystem erfüllt ist, und empfiehlt ein Moratorium für die Einführung des EES, während bestehende Systeme wie das Visa-Informationssystem ausgewertet werden, um zu prüfen, ob die Ziele der EES in angemessener Weise erfüllt werden können.

Da EU-Grossdatenbanken, wie das Registrierungsprogramm für Reisende (RTP) und das Einreise-/Ausreisesystem (EES), das für Grenzkontrollzwecke verwendet wird, die Rechte von EU- und Nicht-EU-Bürgern in Gefahr bringen, von denen ein Teil besonders gefährdet ist, muss die Einführung solcher Datenbanken einer strengen Bewertung unter besonderer Berücksichtigung ihrer Auswirkungen auf die Grundrechte und die Einhaltung des Grundsatzes der Zweckbindung unterzogen werden.

III. Ethische und rechtliche Bewertungskriterien gehen Hand in Hand. Vertrauen kann nur durch ein Zusammenwirken beider Typen von Kriterien (wieder) aufgebaut werden. Daher empfiehlt die EGE verschiedene Massnahmen, um konkreter Vertrauen aufzubauen und die Interessen der Bürger an der Kontrolle über ihre persönlichen Angelegenheiten zu wahren. Diese Massnahmen fallen in die Bereiche Aufsicht, Durchsetzung, Whistleblowing, Information der Öffentlichkeit, Bildung, Ausbildung und Forschung.

12. Vertrauenswürdige Aufsicht

Die EGE erkennt an, dass es in Fragen der nationalen Sicherheit nicht immer möglich ist, mit Blick auf Überwachungsmassnahmen transparent zu sein. Dennoch ist das Vertrauen der Öffentlichkeit von entscheidender Bedeutung für die Legitimität staatlicher Sicherheitsmassnahmen. Zu diesem Zweck empfiehlt die EGE, dass unbeschadet jeglicher gerichtlicher Aufsicht die Mitgliedstaaten eine Stelle oder Person mit Aufsichtsbefugnis einrichten oder die Aufgaben bestehender Gremien erweitern, damit eine vertrauenswürdige dritte Partei zur Verfügung steht, die im Namen der Öffentlichkeit handeln kann. Eine solche Stelle würde auch die Auswirkungen der öffentlichen und privaten Überwachung auf die Rechte und Pflichten der Bürger beobachten. Aggregierte Informationen über die Anzahl der Anträge auf Überwachungsbefugnisse, unabhängig von wem und zu welchem Zweck diese eingereicht wurden, müssen von den Mitgliedstaaten veröffentlicht werden, damit Transparenz und Rechenschaftspflicht gewährleistet sind. Die Mitgliedstaaten sollten eine solche Stelle oder Person im Vorfeld der Einführung von Rechtsvorschriften auf dem Gebiet der Überwachung konsultieren. Die EGE rechnet damit, dass eine solche vertrauenswürdige dritte Partei eine wichtige Rolle bei der Sensibilisierung der Öffentlichkeit und der Anregung von Debatten über

Risiken und Nutzen der Überwachung spielt.

13. Durchsetzung des Datenschutzes

Die EGE ist der Ansicht, dass der im EU-Recht verankerte Datenschutz robust ist, aber auf nationaler Ebene durchgesetzt werden muss. Die Mitgliedstaaten müssen daher sicherstellen, dass die Datenschutzbehörden über ausreichende rechtliche Befugnisse, technisches Know-how und Ressourcen, verfügen, um eine effektive Rechtsdurchsetzung in der gesamten Europäischen Union zu gewährleisten.

14. Whistleblowing

Die Europäische Kommission und die Mitgliedstaaten müssen sicherstellen, dass ein effektiver und umfassender Schutzmechanismus für Whistleblower (Hinweisgeber bzw. Informanten) im öffentlichen wie im privaten Sektor etabliert wird. Im Einklang mit den Grundsätzen von Transparency International, wie im Bericht von 2013 über „Whistleblowing in Europa“ angegeben ist, muss es Vorschriften und Verfahren für Fälle geben, in denen es um die nationale Sicherheit geht, und diese müssen klar sein. Die Vertraulichkeit oder Anonymität muss gewährleistet sein und es muss für gründliche, zeitnahe und unabhängige Untersuchungen der Angaben von Informanten gesorgt werden. Ausserdem muss es transparente, durchsetzbare und zeitnahe Mechanismen geben, um rechtzeitig eine Beschwerde eines Informanten wegen etwaiger Vergeltungsmassnahmen zu verfolgen. Wenn eine Offenlegung Fragen der nationalen Sicherheit, Amts- oder Militärgeheimnisse oder Verschlusssachen betrifft, sind spezielle Verfahren und Garantien für die Berichterstattung einzuführen, die die Sensibilität der Thematik berücksichtigen, um erfolgreich eine interne Verfolgung zu erreichen und eine unnötige externe Exposition zu verhindern. Diese Verfahren sollten eine interne Offenlegung, die Weitergabe an ein autonomes Aufsichtsgremium, das institutionell und operativ unabhängig vom Sicherheitssektor ist, oder die Weitergabe an Behörden mit der entsprechenden Sicherheitsüberprüfung vorsehen. Externe Weitergabe (das heisst, an die Medien und Organisationen der Zivilgesellschaft) würde als letztes Mittel gerechtfertigt werden.

15. Planung von Datenschutz

Behörden und private Unternehmen müssen Planungsprinzipien für den „Datenschutz durch die Entwicklung“ (privacy by design) und den „Datenschutz in der Entwicklung“ (privacy in design) von Sicherheits- und Überwachungstechnologien verabschieden. Die europäischen Werte Würde, Freiheit und Gerechtigkeit müssen vor, während und nach der Gestaltung, Entwicklung und Bereitstellung solcher Technologien berücksichtigt werden. Datenschutzfreundliche Technologien müssen von Anfang an integriert werden, es reicht nicht aus, auf eine spätere Implementierung zu verweisen. Nach Ansicht der EGE ist es möglich, durch die interdisziplinäre Zusammenarbeit von Ingenieuren, Entwicklern und philosophischen und ethischen Experten eine Organisationskultur zu schaffen, in der der Datenschutz verankert ist und in der die gängige Praxis reflektiert wird. Kurse und Schulungen zu ethischen Aspekten auf theoretischer und praktischer Ebene sowohl für Studenten und Hochschulabsolventen in den Fachbereichen Ingenieurwissenschaften und Informatik als auch in der beruflichen Bildung könnten die Berücksichtigung von Datenschutzaspekten bei der Entwicklung von Sicherheits- und Überwachungstechnologien verbessern.

16. Das Verständnis für die Privatssphäre und ihre Wertschätzung

Privatsphäre und Datenschutz sind kein statischen Konzepte, und ein vollständigeres

Verständnis darüber, wie europäische Bürger diese Aspekte verstehen und bewerten, ist unbedingt erforderlich, wenn geeignete Massnahmen ergriffen werden sollen, um die informationelle Selbstbestimmung und den Datenschutz sicherzustellen. Zu diesem Zweck muss die EU Mittel für die Forschung zur Verfügung stellen, um zu untersuchen und zu analysieren, wie Bürgerinnen und Bürger ihre Mitwirkung in Fragen der Sicherheit und Überwachung sehen und pflegen.