Handlungsmöglichkeiten der Schweiz zur Umsetzung und Durchsetzung des Menschenrechts auf Achtung der Privatsphäre

25. August 2013

Die Strafanzeige der Digitalen Gesellschaft wegen PRISM und Tempora dokumentiert massive Menschenrechtsverletzungen betreffend der Privatsphäre von Personen in der Schweiz. Daher ist es dringend notwendig, dass die Schweizer Regierung mit einer umfassenden und wirksamen Strategie dafür sorgt, dass sich diese Menschenrechtsverletzungen nicht fortsetzen können.

Einerseits gehört zu einer solchen Strategie, von den betreffenden Ländern Auskünfte zu verlangen, die (falls wahrheitsgemässe Antworten erteilt werden) es erlauben, den Umfang des Problems abzuschätzen (Punkte 1 bis 4). Die Schweizer Bevölkerung ist über diesen Prozess laufend detailliert zu informieren (Punkt 5). Weiterhin ist abzuklären, ob die nach dem BÜPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs) als Vorratsdatenspeicherung erhobenen Kommunikations-Randdaten der Schweizer Bevölkerung in jedem Fall nur im Inland und mit professionellen Sicherheitsvorkehrungen von hohem Niveau gespeichert werden (Punkte 6 bis 8). Die Speicherung dieser sensiblen Daten unter ungenügenden Sicherheitsvorkehrungen muss jedenfalls für die Zukunft vermieden werden (Punkte 9 und 10), und dies ist auch zu überprüfen (Punkte 11 und 12).

Weiterhin ist die internationale Kooperation mit Regierungen anderer Länder zu suchen, die das Menschenrecht auf Schutz der Privatsphäre ebenfalls ernst nehmen. Im Sinn des Multistakeholder-Ansatzes sind alle Stakeholder, insbesondere Parlament, Bundesamt für Kommunikation (BAKOM) und auch die Zivilgesellschaft und alle im IKT-Bereich tätigen Firmen in die betreffenden Diskussionen einzubeziehen. Dabei muss die Notwendigkeit im Vordergrund stehen, wirksame Strategien und Standards zu entwickeln, damit das Menschenrecht auf Schutz der Privatsphäre im Bereich der Informations- und Kommunikationstechnologien nicht nur theoretisch sondern auch in der Realität gilt (Punkte 13 bis 16).

Internationale Auskunftsbegehren betreffend den Umfang des Problems

1. Die Schweiz muss von den USA Antworten auf folgende Fragen im Hinblick auf Kommunikations-Randdaten verlangen:

a) Haben sich Nachrichtendienste der USA Zugang zu Kommunikations-Randdaten von elektronischer Kommunikation von Personen in der Schweiz – hierzulande, in den USA oder in/durch Drittstaaten – beschafft?

b) Wurde die Informationsbeschaffung im Einzelfall richterlich auf Verhältnismässigkeit in Beziehung zum Menschenrecht auf Achtung der Privatsphäre geprüft?

c) Wie viele Personen in der Schweiz sind von solcher Informationsbeschaffung betroffen?

d) Was ist die Gesamtmenge der betreffenden Kommunikations-Randdaten, in Kilobyte?

2. Die Schweiz muss von den USA Antworten auch auf die analogen Fragen im Hinblick auf Kommunikations-Inhalte verlangen:

a) Haben sich Nachrichtendienste der USA Zugang zu Kommunikations-Inhalten von elektronischer Kommunikation von Personen in der Schweiz – hierzulande, in den USA oder in/durch Drittstaaten – beschafft?

b) Wurde die Informationsbeschaffung im Einzelfall richterlich auf Verhältnismässigkeit in Beziehung zum Menschenrecht auf Achtung der Privatsphäre geprüft?

c) Wie viele Personen in der Schweiz sind von solcher Informationsbeschaffung betroffen?

d) Was ist die Gesamtmenge der betreffenden Daten an Kommunikations-Inhalten, in Kilobyte?

3. Die Schweiz muss vom Vereinigten Königreich Grossbritannien und Nordirland Antworten auf folgende Fragen im Hinblick auf Kommunikations-Randdaten verlangen:

a) Haben sich Nachrichtendienste des Vereinigten Königreichs Grossbritannien und Nordirland Zugang zu Kommunikations-Randdaten von elektronischer Kommunikation von Personen in der Schweiz – hierzulande, in Grossbritannien oder in/durch Drittstaaten – beschafft?

b) Wurde die Informationsbeschaffung im Einzelfall richterlich auf Verhältnismässigkeit in Beziehung zum Menschenrecht auf Achtung der Privatsphäre geprüft?

c) Wie viele Personen in der Schweiz sind von solcher Informationsbeschaffung betroffen?

d) Was ist die Gesamtmenge der betreffenden Kommunikations-Randdaten, in Kilobyte?

4. Die Schweiz muss vom Vereinigten Königreich Grossbritannien und Nordirland Antworten auch auf die analogen Fragen im Hinblick auf Kommunikations-Inhalte verlangen:

a) Haben sich Nachrichtendienste des Vereinigten Königreichs Grossbritannien und Nordirland Zugang zu Kommunikations-Inhalten von elektronischer Kommunikation von Personen in der Schweiz – hierzulande, in Grossbritannien oder in/durch Drittstaaten – beschafft?

b) Wurde die Informationsbeschaffung im Einzelfall richterlich auf Verhältnismässigkeit in Beziehung zum Menschenrecht auf Achtung der Privatsphäre geprüft?

c) Wie viele Personen in der Schweiz sind von solcher Informationsbeschaffung betroffen?

d) Was ist die Gesamtmenge der betreffenden Daten an Kommunikations-Inhalten, in Kilobyte?

Information der Schweizer Bevölkerung über die Diplomatie

5. Die Schweizer Bevölkerung muss über den diplomatischen Prozess der Anfragen an die betreffenden Länder laufend detailliert informiert werden. Schliesslich geht es um fortwährende Verletzungen von Menschenrechten der Schweizer Bevölkerung. Insbesondere sollte die Öffentlichkeit fortlaufend über die diplomatischen Bemühungen orientiert werden, die darauf abzielen, aussagekräftige Antworten auf die Fragen zu erhalten. Auch die eingehenden Antworten sind zu veröffentlichen, und dies auch dann, wenn es sich nur um vorläufige, in der Sache noch nicht wirklich aussagekräftige Antworten handelt.

Von der Vorratsdatenspeicherung nach BÜPF ausgehende Gefahren

6. Weiterhin ist abzuklären, ob die nach dem BÜPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs) als Vorratsdatenspeicherung erhobenen Kommunikations-Randdaten der Schweizer Bevölkerung im Ausland – insbesondere in den USA oder Grossbritannien oder durch Unternehmen die Niederlassungen in den beiden Staaten haben – gespeichert werden. Diese Information kann durch den Dienst ÜPF bei den vom BÜPF betroffenen Providern erhoben werden. Falls es sich dabei herausstellt, dass es Provider gibt, die diese sensitiven Daten im Ausland speichern oder gespeichert haben, sind sie zu verpflichten, die betroffenen Personen über diese Situation zu informieren. Falls es Provider geben sollte, die den Dienst ÜPF nicht darüber informieren, ob die Vorratsdaten im Inland oder im Ausland aufbewahrt werden, muss die Bevölkerung umgehend über diese Situation informiert werden.

7. Aufgrund der durch die Digitale Gesellschaft eingereichte Strafanzeige müssen Staatsanwaltschaft und Polizei untersuchen, ob in der Schweiz tätige Provider allenfalls ausländischen Diensten Zugang zu Randdaten oder Kommunikationsdaten gewähren. Es ist sogar denkbar, dass es dazu schriftliche Verträge geben könnte, siehe etwa diesen Bericht der Washington Post

8. Der Dienst ÜPF muss bei den vom BÜPF betroffenen Providern auch erfragen, wie die als Vorratsdatenspeicherung erhobenen Kommunikations-Randdaten der Schweizer Bevölkerung vor unautorisiertem Zugriff geschützt werden.

9. Für die Zukunft ist die Vorratsdatenspeicherung abzuschaffen.

10. Falls die Vorratsdatenspeicherung nicht abgeschafft wird, sind die Provider, die Kommunikations-Randdaten speichern, wenigstens zu verpflichten, die Daten in der Schweiz zu speichern und dabei ein hohes, präzis definiertes Niveau des Schutzes vor unautorisiertem Zugriff sicherzustellen. Dabei ist ein Informations-Sicherheits-Management-System nach ISO/IEC 27001 zu verwenden.

11. Es muss regelmässig stichprobenartig durch eine Amtsstelle überprüft werden, ob die Pflichten gemäss Punkt 10 zum Schutz der Vorratsdaten vor unautorisiertem Zugriff eingehalten werden.

12. Es muss eine Möglichkeit geschaffen werden, die es unabhängigen Sicherheitsexperten ermöglicht, unter Aufsicht durch eine Amtsperson zu versuchen, die Sicherheitsvorkehrung gemäss Punkt 10 zu umgehen.

Der Weg zu wirksamem internationalem Privatsphäre-Schutz

13. Wirtschaftsspionage und auch die Bespitzelung der Schweizer Bevölkerung durch ausländische Geheimdienste sind nach Schweizer Recht verboten. (Die betreffenden Gesetzesartikel sind in der Strafanzeige der Digitalen Gesellschaft erwähnt.) Damit sind diese Grundrechtsverletzungen aber noch nicht wirksam verhindert, zumal es keine effektiven Mittel zur Durchsetzung dieser Rechtsnorm gibt, wenn die Bespitzelung aus dem Ausland über das Internet erfolgt und mit Duldung oder sogar im Auftrag der Regierung des betreffenden Landes geschieht. Mit Strafbestimmungen, die in der Praxis zum Schutz des Menschenrechts auf Achtung der Privatsphäre ungenügend sind, hat die Schweiz ihre Pflichten im Rahmen der internationalen Menschenrechtsabkommen offensichtlich noch nicht erfüllt.

14. Folglich ist die Schweiz aus Menschenrechtsperspektive sogar zwingend verpflichtet,

weitere Massnahmen zu ergreifen. Es drängt sich insbesondere auf, dass das Bundesamt für Kommunikation die Entwicklung und Umsetzung von technischen Standards zum Schutz von Kommunikations-Randdaten und -Inhalten durch Verschlüsselung fördern und durchsetzen muss.

15. Regierung und Parlament stehen in der Verantwortung, unter Einbeziehung von externen Fachleuten eine nationale Strategie zur Lösung dieser Probleme zu erarbeiten. Dabei ist es von grossem Vorteil, wenn diese Strategieerarbeitung in einem international koordinierten, transparenten und insbesondere auch für internationale NGOs mit Kompetenzen im Menschenrechtsbereich zugänglichen sogenannten Multistakeholder-Prozess stattfinden kann. Wir schlagen hierfür den WisdomTaskForce Ansatz vor.

16. Aktuell gibt es unter dem Namen „Enhanced Cooperation Working Group“ eine Arbeitsgruppe der Vereinten Nationen , die unter anderem zu analysieren versucht, was die wichtigen Themen für verbesserte internationale Kooperation im Internet Governance Bereich sind. Die Schweiz ist Mitglied dieser Arbeitsgruppe. Wir fordern die Schweizer Regierung auf, hier unbedingt zu fordern, dass „Internationale Kooperation zur Umsetzung des Menschenrechts auf Achtung der Privatsphäre im IKT-Kontext“ ganz oben auf die Liste gesetzt wird. Weiterhin sind die verschiedenen diplomatischen Möglichkeiten etwa am Rand der Sitzungen der Enhanced Cooperation Working Group und im Rahmen des Internet Governance Forums aktiv zu nutzen, um die Regierungen möglichst vieler Länder zur Mitarbeit an einer erfolgversprechenden Lösungsstrategie zu gewinnen.