

- Bewaffnete Drohnen im Einsatz kreisen lange Zeit hör- und sichtbar über Gebiete, die in aller Regel bewohnt sind. Für die betroffene Zivilbevölkerung ist das permanenter psychologischer Terror. Die psychologische Belastung ist für die Drohnenpilotinnen und -piloten sowie für die weiteren Entscheidungsträger nicht minder gravierend, weil sie das Abfeuern der Waffen auf der Basis von Bildern entscheiden müssen, die automatisch aufbereitete Ziele zeigen, deren Interpretation alles andere als eindeutig ist.
- Bewaffnete Drohnen, deren Bodenstationen aus erfolgreicher Drohnen, bei denen nicht nur die Steuerung erfolgt, sondern auch die Entscheidung über Tod und Leben der Programmierung der Bordcomputer verlegt. Aus unserer fachlichen Sicht scheint es unmöglich zu sein, Entscheidungsprogramme zu entwickeln, die das völkerrechtskonform leisten können. Dessen ungeachtet wird aber intensiv an der Entwicklung autonomer Waffen gearbeitet. Und wenn solche Waffen verfügbar sind, was ist dann das Bekenntnis der Bundesregierung wert, niemals autonome Waffen einzu-

erschienen in der *Fiff-Kommunikation*,  
herausgegeben von *Fiff e.V.* - ISSN 0938-3476  
[www.fiff.de](http://www.fiff.de)

setzen, wenn Stimmen laut werden, dass sie für den Schutz der Soldatinnen und Soldaten gebraucht werden?

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Fiff) beschäftigt sich seit seiner Gründung 1984 mit den gesellschaftlichen Auswirkungen von Informatik und Informationstechnik, wobei die unheilvolle Verquickung von Rüstung und Informatik ein wesentliches Thema ist. Bewaffnete Drohnen und sonstige unbemannte Waffensysteme sowie deren absehbare Autonomisierung sind aktuelle Themen. Der Beitrag der Informatik nicht nur die Welt nicht sicherer, sondern die Spirale weiter an und bergen die Hände zu geraten. Ein Verbot der Entwicklung von autonomen Waffen ist aus unserer Sicht die richtige Alternative. Wir bitten Sie, sich nach Kräften für die Verwirklichung einzusetzen.

Mit freundlichen Grüßen

Hans-Jörg Kreowski  
im Namen des Fiff-Vorstands



Fiff e.V. – Pressemitteilung

## Sachverständigenauskunft zur Digitalisierung von Verwaltungsverfahren bei Familienleistungen

3. November 2020 – *Schlecht durchdachter Entwurf macht kleine Schritte hin zur Digitalisierung von Verwaltungsverfahren, aber in die falsche Richtung. Zudem werden ganz nebenbei wesentliche Änderungen am Online-Zugangs-Gesetz vorgenommen.*

Vor einer Woche fand eine Sachverständigenanhörung im Innenausschuss des Bundestages statt, zu welcher auch das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Fiff) geladen war. In Person von Rainer Rehak legten wir unsere Ansicht zum **Gesetzesentwurf der Bundesregierung zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen** sowohl mündlich als auch schriftlich dar.

Die Bestrebungen, Verwaltungsleistungen neben anderen Wegen auch digital und online anzubieten, sind auch unserer Ansicht nach grundsätzlich zu befürworten. Dabei ist besonders die konkrete Zielstellung, dass „die Papierformulare aber nicht einfach nur in eine digitale Form gebracht und auf elektronischem Wege an die Behörde gesendet werden, sondern die Potenziale der Digitalisierung für die Abwicklung der Verwaltungsprozesse gehoben werden“ sollen, hervorzuheben und sehr zu begrüßen. Ein derartiges Vorhaben kann dabei viele Vorteile für die Verwaltung selbst und vor allem für die BürgerInnen und Organisationen bedeuten. Demnach ist der Gegenstand unserer Stellungnahme nicht die defensive Frage nach dem *Ob*, sondern die gestalterische Frage nach dem *Wie* einer solchen digitalen Transformation.

### Kritische Analyse

Leider fällt die konkrete Ausgestaltung des digitalen Angebots von Familienleistungen, so wie sie im Gesetz inklusive Ände-

rungsantrag angelegt sind, nicht nur weit hinter die zuvor ausgegebene Losung zurück, sondern erzeugt zusätzlich gravierende Probleme hinsichtlich Datenschutzfragen beim E-Government sowie bezüglich der perspektivischen Weiterentwicklung und Interoperabilität digitaler Verwaltungssysteme.

*„Entgegen den Beteuerungen von BürgerInnenfreundlichkeit und Hebung digitaler Potenziale ist das vorgesehene System Ergebnis einer sehr speziellen Verwaltungsdenkweise, in der die AntragstellerInnen zwar von außen ein monolithisches System in Gang setzen können, jedoch ab diesem Moment keinerlei Einsichts-, Interaktions- oder gar Interventionsmöglichkeiten mehr besitzen, während sich die inneren Elemente des Systems wiederum gegenseitig blind vertrauen.“*

kommentiert Rainer Rehak, Datenschutzexperte des Fiff.

*„Diese staatliche Vertrauens-Community, die sich mangels Interoperabilität nach ‚außen‘ verbarrikadiert, ist ein Frontalangriff auf die eigentlich gebotene informationelle Gewaltenteilung des Staates.“* führt Kirsten Bock, Datenschutzexpertin des Fiff, weiter aus.

Wir kritisieren die folgenden Punkte, die sich auf die angelegten Funktionen, die geplante technische Umsetzung und spezielle Datenschutzfragen beziehen. In unserer Stellungnahme finden

sich jeweils konstruktive Vorschläge, wie unsere Kritik von der GesetzgeberIn fruchtbar gemacht werden kann. Folgende Kernkritikpunkte werden in dieser Stellungnahme behandelt:

1. Die Schaffung einer isolierten Behördeninsel, die nach außen hin – auch den BürgerInnen gegenüber – abgeschottet ist und innerhalb der Verwaltung zwischen den Behörden keinerlei Beschränkungen unterliegt, ist mindestens aus Datenschutz-, IT-Sicherheits- und Interoperabilitätsgesichtspunkten hochproblematisch.
2. Sichere Kommunikation zwischen BürgerInnen und Behörden ist auch mit den nun geregelten neuen Postfächern nicht möglich, sie sind nämlich Einbahnstraßen behördlicher Kommunikation und nicht abgesichert, wegen der auch schon bei De-Mail fatalen „Zustellfiktion“ wenig attraktiv und nur umständlich nutzbar.
3. Interoperabilität wurde an vielen Stellen ignoriert. Weder beim Abruf der Postfächer noch bei der Spezifikation der Postfächerfunktionen wurde auf bewährte Standards gesetzt (IMAP, eDelivery etc.), die eine Verbindung mit anderen Systemen, etwa mit EU-Behörden, der Verwaltung anderer Länder oder den Systemen der BürgerInnen grundsätzlich ermöglicht hätte.
4. Die Nutzung eines eindeutigen Personenkennzeichens, beispielsweise der Steuer-Identifikationsnummer (StID), wird unserer Ansicht nach implizit vorausgesetzt, mindestens aber nicht explizit abgelehnt. Da bereichsspezifische Kennzeichen die gleiche Funktionalität erlauben, sind diese grundsätzlich zu verwenden und eindeutige Personenkennzeichen abzulehnen. Dies ist auch aus Akzeptanzgründen der zu wählende Weg.
5. Im Entwurf fehlt ein zentrales Element von E-Government: Eine qualifizierte elektronische Signatur (QES) etwa zur Signierung von Dokumenten sowohl durch Behörden aber auch durch BürgerInnen, mit welcher signierte Nachrichten oder digitale Urkunden etc. ausgestellt werden könnten.
6. Ebenfalls stark kritikwürdig erscheint uns der Ansatz, die ursprünglich nur für die Steuerübermittlung gedachten ELS-TER-Zertifikate für die Authentifizierung von Organisationen am Portalverbund (PV) zweckzuentfremden. Ein System

mit derartig schwachen Sicherheitseigenschaften wie etwa einem Zwei-Faktor-Mechanismus basierend auf der Zertifikatsdatei und einer PIN taugt nicht (auch nicht provisorisch) als organisationale Authentifizierung für jegliche staatliche Leistungen.

Zuletzt sei an dieser Stelle auch eine parlamentarische Prozesskritik erlaubt. Einerseits ist das zentrale und komplexe Funktionselement der sogenannten Verwaltungspostfächer erst im nachgereichten Änderungsantrag zu finden, andererseits umfasst der vorgelegte Entwurf auch ganz nebenbei diverse tiefgreifende Änderungen am zentralen Online-Zugangs-Gesetz (OZG). Dadurch wird offensichtlich, dass hier weder thematisch umsichtig noch gesetzgeberisch systematisch vorgegangen worden ist, was gerade bei der Planung von (digitalen) Infrastrukturen – also der Erzeugung enormer Pfadabhängigkeiten – dringend geboten wäre.

Auch wenn die Gewährung von Familienleistungen nur ein erster Schritt bei der Digitalisierung von Verwaltungsverfahren ist, so werden hier dennoch Grundlagen auch für weitere Leistungen gelegt. Nötig ist hier – im Gegensatz zum aktuellen Entwurf – eine langfristige Planung und Perspektive, sonst stellen sich die oben angerissenen Fragen und Probleme in ein paar Jahren wieder, dann aber mit bereits geschaffenen Tatsachen, die im Wege stehen. Noch kann der Kurs korrigiert werden und sollte dies auch.

*„Die Digitalisierung im 21. Jahrhundert sollte Demokratie und Rechtsstaat krisensicher machen. Der Bundesregierung gelingt dies mit dem vorgelegten Entwurf nicht, im Gegenteil“, fasst Kirsten Bock zusammen.*

## Referenzen

- [1] Die FfF-Stellungnahme: [https://www.fiff.de/presse/FfF\\_Sachverstaendigenauskunft\\_Digitale%20Familienleistungen.pdf\\_at\\_download/file](https://www.fiff.de/presse/FfF_Sachverstaendigenauskunft_Digitale%20Familienleistungen.pdf_at_download/file)
- [2] Gesetzesentwurf der Bundesregierung: <https://dip21.bundestag.de/dip21/btd/19/219/1921987.pdf>
- [3] Änderungsantrag der Fraktionen SPD/CDU/CSU : <https://www.bundestag.de/resource/blob/800342/bfe0e515ef0b44adc48744931ff170ab/A-Drs-19-4-587-data.pdf>
- [4] Webseite der Anhörung inklusive Aufzeichnung der mündlichen Befragung: <https://www.bundestag.de/dokumente/textarchiv/2020/kw44-pa-inneres-familienleistungen-800334>



FfF e. V. – Pressemitteilung

## Aushebelung von Ende-zu-Ende-Verschlüsselung trifft die Falschen und leistet der IT-Sicherheit einen Bärendienst

10. November 2020 – EU-Ministerrat strebt praktisch ein Verbot von Ende-zu-Ende-Verschlüsselung an, einem elementaren Baustein der vertrauenswürdigen digitalen Gesellschaft, dabei haben „haarsträubende Ermittlungsfehler bei den Behörden den Anschlag in Wien erst ermöglicht, nicht fehlende digitale Überwachungsbefugnisse“ (Erich Möchel).

Der EU-Ministerrat veröffentlichte am 6. November 2020 das überarbeitete Entwurfspapier „Draft Council Declaration on Encryption – Security through encryption and security despite en-

ryption“ [1]. Darin berichten die AutorInnen von der Absicht, einen gesetzlichen Rahmen zu schaffen, durch den AnbieterInnen von Messenger-Diensten wie Signal, Threema, Telegram,