WIEN / 23. März 2020 *

SMS-Warnsystem

Bewertung der Einführung eines Warnsystems, das die Bevölkerung via SMS oder Anruf vor drohenden Gefahren warnt

Änderung des Telekommunikationsgesetz 2003

Für epicenter.works

Lisa Seidl, LL.M

Mitarbeit:
Benedikt Gollatz
Dipl.-Ing. Dr. Walter Hötzendorfer

EPICENTER .WORKS
for digital rights

*Update 31.3.2020

ÄNDERUNG DES TELEKOMMUNIKATIONSGESETZ 2003:

Die Bundesregierung verpflichtet nun Telekommunikationsunternehmen[1], der Bevölkerung öffentliche Warnungen vor drohenden oder sich ausbreitenden größeren Notfällen und Katastrophen oder damit im Zusammenhang stehende Aufrufe per SMS zuzusenden. Diese neue Art, die Bevölkerung zu informieren, könnte – je nachdem wie personenbezogenen Daten verarbeitet werden – in Konflikt mit dem **verfassungsrechtlich gewährleisteten Grundrecht auf Datenschutz** stehen:

Grundsätzlich dürfen Stamm- und Standortdaten, also personenbezogene Daten, nur verarbeitet werden, wenn es für Warnungen vor drohenden oder sich ausbreitenden größeren Notfällen und Katastrophen oder für damit im Zusammenhang stehende Aufrufe für ein legitimes Ziel erforderlich ist. So sollen Warnungen und Aufrufe an Endnutzer*innen gesendet werden, „unabhängig von ihrem Wohnort […] die sich im fraglichen Zeitraum in den möglicherweise von den drohenden oder sich ausbreitenden größeren Notfällen und Katastrophen betroffenen geografischen Gebieten […] aufhalten". Das Ziel ist, Menschen mit leicht zugänglichen Mitteln zu warnen.

Dabei können unterschiedliche personenbezogene Daten verarbeitet werden. Handelt es sich nur um Stammdaten (zB Alter, Kunden*innenadressen), die ausschließlich vom Telekomanbieter verarbeitet und nicht weitergegeben werden, ist die Verarbeitung relativ unbedenklich, da der **Grundrechtseingriff zum verwendeten Mittel verhältnismäßig ist**.

Nur Momentaufnahmen erlaubt, keine Vorratsdatenspeicherung

Bei der Verarbeitung von Standortdaten muss man hinsichtlich der Aktualität unterscheiden: In verfassungskonformer Interpretation des § 98a TKG dürfen nur Standortdaten von Personen verarbeitet werden, die sich aktuell im betroffenen Gebiet aufhalten (zB in einer Funkzelle eingeloggt sind).

Eine Verarbeitung von Standortdaten von Personen, die in der Vergangenheit in einem bestimmten Gebiet waren (zB in einer Funkzelle eingeloggt waren) wäre verfassungswidrig. Denn dafür müssten die Telekommunikationsanbieter diese Daten länger als für den Betrieb der Dienstleistung notwendig speichern, um diese Daten im Fall einer Anfrage durch die Behörden - unter sonstiger Androhung einer mit bis zu 37.000,- EUR bedrohten Strafe - zur Verfügung zu haben. Diese Verarbeitung wäre als **Vorratsdatenspeicherung** zu klassifizieren, welche durch VfGH und EuGH als verfassungs- bzw. grundrechtswidrig eingestuft[2] wurde.

Auch rechtfertigt die derzeitige Situation keine Ausnahme, insbesondere da die Standortdaten zu ungenau sind und nicht auf eine Infektion schließen lassen. Diese Maßnahme stellt somit kein geeignetes Mittel dar, um das Ziel der öffentlichen Gesundheit zu erreichen. Eine unterschiedslose Vorratsdatenspeicherung, die jedenfalls und ohne konkreten Anlassfall und ohne richterliche Anordnung oder Anordnung einer unabhängigen Verwaltungsbehörde vorgenommen wird, ist überschießend und ein Mittel, das nie verhältnismäßig zum Grundrechtseingriff sein kann. Insbesonders schwerwiegend ist hier, dass diese Praxis bei allen Personen ein Gefühl erzeugt, dass das eigene Privatleben Gegenstand einer ständigen Überwachung ist.

1 https://www.ris.bka.gv.at/eli/bgbl/i/2003/70/P98a/NOR40221485
2 https://epicenter.works/thema/vorratsdatenspeicherung

Es fehlt eine gesetzliche Klarstellung, welche Art von Standortdaten (aktuell oder historisch) zu verarbeiten sind. Diese wäre dringend notwendig.

Wenn auch die Betroffenen nicht – wie so oft im Datenschutzrecht üblich – über die Verarbeitung ihrer Daten informiert werden müssen, ist jedenfalls begrüßenswert, dass diese Information zumindest über die Website der Rundfunk- und Telekom Regulierungs-GmbH (RTR) veröffentlicht wird.

Dass die vorliegende Regelung – da sie jedenfalls sehr eingriffsintensiv hinsichtlich des Grundrechts auf Datenschutz ist – nur bis 31.12.2020 in Kraft ist, ist zu befürworten.