Evaluación de impacto relativa a la protección de datos para la app de corona

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
demian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Měto R. Ost
meto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.2 – 17 de abril de 2020

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.

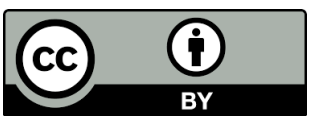
Contact: dsfa-corona@fiff.de

https://www.fiff.de/dsfa-corona

https://www.fiff.de/dsfa-corona

Version 1.2 (ES) published 17 de abril de 2020.
Version 1.0 (DE) published April 14, 2020.

Document available here:
https://www.fiff.de/dsfa-corona



Resumen y resultados

Desde el inicio de la expansión del virus SARS-CoV-2 en Europa a principios del 2020 ha aparecido una visión tecnológica que marca el debate político y público en general. Esa visión manifiesta que posiblemente se podría contener la expansión de la pandemia que nos afecta mediante el uso de Tracing-Apps o aplicaciónes de localización desarrolladas para los teléfonos inteligentes. Este sistema registraría de forma automatizada los contactos entre personas usuarias de esos teléfonos y de esa forma permitiría comprender más rapido y eficiente las cadenas de infección y posibilitando el aislamiento anticipado de personas afectadas.

Algunos estados como Singapur, Corea del Sur e Israel han en parte presentado ejemplos radicales de la aplicación para este procedimiento, que desde el punto de vista de los sistemas legales europeos se consideran como limitaciones excesivas de los derechos fundamentales de los ciudadanos. Como reacción se han formado diferentes iniciativas en Europa, especialmente el consorcio *Pan-European Privacy Preserving Proximity Tracing* (PEPP-PT), que toma el concepto de una Corona Tracing App y que ya en su denominación plantea un compromiso con la Protección de Datos o como mínimo con la *Privacy* (conviene recordar que esos dos términos no son sinónimos). De esta forma se están desarrollando sistemas de seguimiento que en comparación con las medidas utilizadas en países no europeos son más adecuadas en materia de Protección de Datos. En los medios se ha propagado una imagen que transmite que las Corona-Apps *made in Europe* prometen proteger la «esfera privada» de los usuarios y ser adecuadas a la normativa establecida por el Reglamento General de Protección de Datos.

El ser «Data Protection friendly» o en castellano ser pro Protección de Datos no es una cuestión que permita ser respondida directamente con un sí o con un no, sino que es una consideración compleja que requiere una discusión precisa y detallada. EL RGPD obliga a los responsables de tratamientos de datos personales a gran escala (categoría a la que sin duda pertenece un sistema como el que nos ocupa, ver capítulo 6) a desarrollar una evaluación del impacto sobre la Protección de Datos en el caso de existir un riesgo alto para los derechos y libertades de los sujetos afectados. Esa evaluación supone un estructurado análisis de riesgos que debe identificar y valorar con antelación las consecuencias que un tratamiento de ese tipo puede tener.

Los sistemas de Corona-Tracing que nos ocupan suponen un enorme experimento social bajo control estatal de registro digital del comportamiento humano en Europa. La efectividad y las consecuencias de estas aplicaciones no son todavía previsibles y es de suponer que en la UE se probarán y evaluarán diferentes variaciones de esos sistemas. Las consecuencias en materia de Protección de Datos, y en consecuencia en materia de derechos fundamentales, de estas iniciativas afectan potencialmente no solo a sujetos individuales, sino a la sociedad en su conjunto. Por estos motivos parece necesario no solo la elaboración de una evaluación del impacto sobre la Protección de Datos, sino especialmente su publicación y una posterior discusión al respecto. Dado que hasta ahora ninguna de las instituciones implicadas ha hecho pública una evaluación de impacto como la que nos ocupa y que los **privacy impact assessments** que se han presentado son incompletos, nosotros – un grupo de investigadores y expertos en

Protección de Datos en el *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF, foro de informaticxs por la paz y la responsabilidad social) e. V.* – hemos decidido por medio de este documento presentar una evaluación de impacto sobre la Protección de Datos como aportación constructiva.

Resumen sobre el procedimiento

En esta evaluación de impacto sobre la Protección de Datos nos referimos a los marcos y conceptos de diseño que actualmente están siendo principalmente discutidos como adecuados para una Corona-Tracing-App europea. Esa App estaría basada en una tecnología de sensores de proximidad por medio de Bluetooth Low Energy (BTLE). Entre ellos cabe destacar PEPP-PT[1], DP-3T[2], así como un concepto general resumido por el miembro del *Chaos Computer Club* Linus Neumann[3]. Entre estos proyectos PEPP-PT presenta un marco conceptual, no una App concreta sino una especificación para un sistema de tratamiento de datos de este tipo. Dentro de ese marco son imaginables diferentes implementaciones, es decir sistemas o Apps, que harían realidad ese marco conceptual. El PEPP-PT como marco conceptual permitiría en principio que cada nación en Europa desarrollara su propia implementación del mismo. De esa forma ofrece un margen de maniobra, mientras que al mismo tiempo pretende garantizar una interoperabilidad transfronteriza.

En esta situación uno de los principales resultados de nuestra investigación es que todos los marcos analizados, y especialmente el PEPP-PT, **dejan sin concretar importantes características de la tecnología y del procedimiento que están relacionadas con consecuencias relevantes en materia de Protección de Datos**. A groso modo se pueden diferenciar como mínimo tres arquitecturas de sistemas que serían compatibles con el marco conceptual del PEPP-PT (ver capítulo 1):

a) **Una arquitectura centralizada** en la que la anonimidad de los usuarios y la confidencialidad de los casos de contacto solo se persigue con efectos hacia el exterior, es decir frente a otros usuarios y frente a actores externos. Los responsables de la plataforma y las administraciones participantes pueden identificar a todos los usuarios y relacionarlos con el historial de contactos.

b) **Una arquitectura parcialmente descentralizada** que al mismo tiempo permite la **investigación epidemiológica** (DP-3T) en la que los usuarios y el historial de contactos solo son confidenciales frente a otros usuarios y frente a terceros, mientras que el servidor puede personalizar los datos de los usuarios infectados. El sistema dispone de una función de donación de datos por medio de la cual los usuarios pueden poner a disposición del sistema su historial de contactos para la realización de investigaciones epidemiológicas. En esos casos los historiales de contactos de los usuarios infectados son accesibles para los responsables de la plataforma y para las administraciones implicadas.

c) **Una arquitectura totalmente descentralizada.** Frente a otros usuarios y frente a terceros los usuarios permanecen anónimos y el historial de contactos es

[1] Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (2020). URL: `https://www.pepp-pt.org/` (visitado 08-04-2020)

[2] Carmela Troncoso y col. (2020). *Decentralized Privacy-Preserving Proximity Tracing*. White Paper Version: 10th April 2020

[3] Linus Neumann (2020). *«Corona-Apps»: Sinn und Unsinn von Tracking*. URL: `https://linus-neumann.de/2020/03/corona-apps-sinn-und-unsinn-von-tracking/` (visitado 09-04-2020)

confidencial. Los responsables de la plataforma y las administraciones implicadas pueden desanonimizar los datos de los usuarios infectados pero no sus historiales de contactos. Las investigaciones epidemiológicas no son apoyadas por esta solución.

Responsable y administración pueden ...	Variante a)	Variante b)	Variante c)
... desanonimizar los datos de todos los usuarios	Sí	No	No
... desanonimizar los datos de usuarios infectados	Sí	Sí	Sí
... reconocer todos los contactos	Sí	Parcialmente	No

Nuestra evaluación de impacto se centra principalmente en la variante c, la más «amigable» en materia de Protección de Datos, revisaremos parcialmente los detalles técnicos de la variante b.

Los resultados muestran que, en primer lugar, incluso **la arquitectura totalmente descentralizada muestra numerosos y graves vulnerabilidades (ver capítulo 7) así como riesgos** que deben ser enfrentados. En segundo lugar la comparación entre las variantes centralizadas y descentralizadas muestra, que realizamos en puntos relevantes, que **decidirse por una de estas dos variantes tiene consecuencias relevantes en materia de Protección de Datos.** Afirmar que cualquier implementación de la PEPP-PT es «amigable» con la Protección de Datos no es correcto de forma generalizada.

Principales resultados, riesgos y posibles soluciones

A continuación presentamos los principales resultados, riesgos y posibles soluciones:

1. **La voluntariedad del uso de la App tan a menudo mencionada en las discusiones sobre el tema es una ilusión.** Es imaginable, y de hecho ya se discute sobre este tema, que el uso de la App podría ser un requisito para la relajación de las condiciones individuales en materia de restricciones de movimientos. El ser capaz de mostrar la condición de usuario de la App podría actuar como condición para el acceso a edificios, instalaciones o eventos. Es también imaginable que los empleadores adaptarían rápidamente estas medidas porque de esa forma podrían reabrir sus negocios por medio de una medida de protección voluntaria. Este escenario supone una coacción implícita para el uso de la App y supone una discriminación o trato desigual de quienes no la utilizan. Dado que no todo el mundo posee un teléfono inteligente, la implementación del sistema supondría también una discriminación para grupos ya desfavorecidos por otros motivos.

2. **Si no se garantiza la capacidad de intervenir y una finalidad del tratamiento claramente restringida, la protección de los derechos fundamentales está claramente en peligro.** Por ejemplo existe un alto riesgo de falsos registros de exposición al virus (falsos positivos), que tendrían como consecuencia un autoconfinamiento o una cuarentena (por ejemplo el registro de un

contacto a través del muro entre dos viviendas). Para poder enfrentarse a este problema es preciso garantizar tanto desde el punto de vista legal como técnico la posibilidad de actuar de forma efectiva sobre los datos, por ejemplo para hacer retirar declaraciones de infección erróneas, el borrado de registros equivocados de contacto con una persona infectada o la impugnación de restricciones aplicadas en base al tratamiento de datos en la App. Hasta el momento ninguno de los sistemas propuestos plantea esta posibilidad.

3. **Todos los procedimientos mencionados hasta el momento tratan datos de salud.** El procedimiento se basa en el tratamiento de datos en los teléfonos inteligentes, el envío de esos datos a un servidor después del diagnóstico de una infección y finalmente su distribución al resto de teléfonos inteligentes para proceder al control de un posible contacto con personas infectadas. Todos los datos disponibles en un teléfono inteligente son personales, están relacionados con el usuario de ese teléfono. Dado que solo se transmiten los datos de las personas diagnosticadas como infectadas, los datos transmitidos son datos de salud. Por lo tanto deben gozar de la protección prevista en el RGPD.

4. **La anonimidad de los usuarios debe garantizarse por medio de una combinación de medidas legales, técnicas y organizativas.** Solo por medio de un enfoque multidimensional se puede garantizar que los datos no podrán ser personalizados de nuevo, de forma que realmente se pueda hablar de datos anonimizados. Todas las propuestas presentadas hasta ahora carecen de un procedimiento explícito de separación de los datos. En esta evaluación de impacto sobre la Protección de Datos hemos formulado exigencias legales, técnicas y organizativas cuya aplicación en la práctica garantizaría una separación efectiva e irreversible. Solo con estas condiciones los datos referentes a infecciones pueden ser utilizados y distribuidos entre las Apps.

La perspectiva de la Protección de Datos parte de la idea que **los principales riesgos del tratamiento de datos personales provienen del responsable del sistema de tratamiento**.

En casos como el que nos ocupa es imprescindible que las barreras para un tratamiento abusivo de los datos que vaya más allá de la finalidad establecida estén formadas por una combinación efectiva de medidas legales, técnicas y organizativas y no pura y simplemente por promesas vacías de los responsables en el sentido de respetar la normativa de Protección de Datos. Las mencionadas medidas deben estar correctamente documentadas y ser controlables.

El desarrollo abierto de los sevidores y Apps junto con todos sus componentes, por ejemplo utilizando Software Libre, es una condición esencial para garantizar **la transparencia de los principios generales de la Protección de Datos** no solo para las Autoridades de Protección de Datos sino también, y especialmente, para los sujetos afectados y para la sociedad en general. Solo de esa forma se puede conseguir la confianza de los afectados, también en el caso de aquellos afectados que no conocen con detalle los aspectos técnicos de las tecnologías de la información.

Terceros ajenos a la organización también pueden generar riesgos para los derechos fundamentales. No hay que pensar en primer lugar en Hackers, mejor dicho Crackers, sino en **actores con fines comerciales** como grandes plataformas y en organizaciones estatales. Esas organizaciones pueden sacar provecho de la ingente cantidad de datos de localización, que ellos mismos pueden analizar, ya que Bluetooth debe estar permanentemente activado para que la Corona App funcione. También podrían acceder por

diferentes vías a los datos almacenados por los usuarios.

Los análisis de Protección de Datos consideran el tratamiento de datos en su conjunto y no solo las Apps utilizadas.

En la discusión pública sobre el tema y en los proyectos de Apps seleccionados se reduce el tema de la Protección de Datos a la protección de la esfera privada, a la protección del secreto frente a responsables de tratamiento y a terceros, y a los aspectos de la seguridad de la información como la encriptación. Con esta visión reducida del problema los significativos riesgos, tanto políticos como sociales, que intentamos mostrar en esta evaluación de impacto no solo son ignorados sino que incluso se podría decir que son ocultados.