La digitalización en tiempos de (pos)pandemia: poner el ojo sobre la lupa

La pandemia exhibió drásticamente problemáticas que ya estaban latentes para la gestión de datos y la seguridad digital. El aumento de ataques y las nuevas situaciones que se han generado por la aparición, popularización y difusión de interacciones virtuales traen aparejadas consecuencias para los ciudadanos: desde exposición a delitos hasta el manejo arbitrario de la información por parte de los actores más poderosos en el mundo digital. Usar los datos para el bien público requiere gestionarlos adecuadamente y asegurar la privacidad.

Durante la pandemia hemos asistido a un incremento inédito de la digitalización en casi todos las actividades y franjas etarias: educación, trabajo, ocio, trámites, redes sociales y comunicación en general, tanto para niños/as, como para adolescentes y adultos/as. Aumentaron también, en paralelo y de manera notable, los problemas de seguridad en el mundo digital. Sin embargo, la defensa de los datos y de la privacidad no se optimizaron en forma proporcional: quedó en evidencia que los datos surgidos de la interacción de los ciudadanos con organizaciones públicas y privadas son críticas y su seguridad es endeble. En este documento, nos concentramos en las interacciones de los ciudadanos con el Estado.

MENSAJES CLAVE

- La pandemia dejó claro que no utilizar los datos para diseñar y ejecutar políticas públicas es negligencia: la gestión de datos, en aquellos casos en que se realizó de forma eficiente, contribuyó a salvar vidas. No usar los datos está fuera de discusión.
- Se verificó un enorme crecimiento en el uso de aplicaciones que manejan datos sensibles, como *apps* de salud o financieras (desde billeteras virtuales hasta *apps* de bancos).
- Con el trabajo remoto o híbrido, se produjo un aumento enorme en el intercambio de información digital, sin correlato alguno en la implementación de medidas que acompañen la privacidad y la seguridad de esos datos.
- Hubo controles a nuestra movilidad (datos que se analizaron para entender el efecto de los aislamientos y evaluar políticas públicas), *apps* obligatorias o voluntarias (para circular, identificarse, acceder a servicios, solicitar permisos, incluso de *self-reporting*), rastreo de contactos estrechos, seguimiento de casos, y hasta análisis de nuestros desechos (análisis de aguas servidas).
- Todos los niños y adolescentes estuvieron mucho más tiempo *online*. La educación se pasó a modalidad virtual, lo que de por sí generó una cantidad enorme de información.
- La masa crítica de información generada durante la pandemia fue también objeto de hackeos o robos de información cuyos alcances y consecuencias no conocemos. Esto ocurrió en el sector privado, pero también en el Estado: los casos Renaper y Senado, si bien con escasos detalles, salieron a la luz.
- Aumentaron delitos digitales: *malware*, estafas virtuales, ataques a la privacidad, robo de identidad, robo de información, secuestro de datos (*ransomware*).
- Emergió como fenómeno autóctono de la pandemia el *zoom bombing*: el ingreso no autorizado a sesiones interrumpiendo con contenido poco apropiado o ruido. Un ejemplo ilustrativo de la importancia de este fenómeno es que llevó a que se iniciaran acciones legales contra la empresa Zoom en California, en un juicio en el que se llegó a un acuerdo por 85 millones de dólares como compensación por violaciones a la privacidad.
- A pesar de la producción de este caudal de información, en algunos casos bastante sensible, no hubo ningún cambio en la regulación argentina de la privacidad, datos personales o intercambio de datos, desde el inicio de la pandemia hasta la actualidad, profundizando una deuda normativa existente desde antes de la pandemia.
- La inexistencia de regulaciones claras y de leyes que indiquen claramente cuándo y cómo está permitido el uso de los datos ha llevado a que se evite cualquier intercambio de datos, se busquen soluciones de "seguridad perfecta" o se busquen alternativas al análisis cuantitativo, e incluso a que se descarte la evidencia como algo necesario al proponer políticas públicas. La parálisis es el peor de los escenarios.

Aportes de políticas públicas

- El gobierno de datos debe definir reglas claras para el intercambio de datos entre los ciudadanos y el Estado, sobre todo para los datos que los ciudadanos entregan a los organismos públicos. Para esto, debe establecer políticas y programas que describan cómo se debe cuidar y gestionar los datos de los ciudadanos.
- La seguridad informática en el Estado debe ser priorizada, en particular en lo relativo a la identificación segura de los ciudadanos. Es fundamental abandonar sistemas de verificación vulnerables como el número de trámite del DNI y avanzar en esquemas más seguros (biométricos, de 2 pasos, etc). Esta priorización debe traducirse en capacitación a funcionarios e inversión en seguridad informática.
- Se debe exigir a todas las dependencias que la información sensible sea adecuadamente encriptada y que solo se solicite la realmente necesaria. También, que se implementen mayores niveles de seguridad, sobre todo en el acceso a trámites o interacciones obligatorias, y en situaciones que configuran contratos de adhesión.
- Se debe tener en cuenta que parte de la población tiene pobre acceso a medios digitales o no está alfabetizada digitalmente: el gobierno de datos debe considerar la brecha digital y proveer mecanismos para acompañar a quienes tienen dificultades para el acceso.
- El gobierno de datos debe proveer las bases para desarrollar pautas éticas para el uso de datos, algoritmos e inteligencia artificial en el sector público. No obstante, es improbable, que una iniciativa de uso ético de inteligencia artificial y algoritmos prospere sin tener antes definida la gestión y la gobernanza de los datos.
- Las y los ciudadanos debe tener control sobre el uso que se hace de sus datos y no ser despojados de ese derecho por omisión o por el mero paso del tiempo: el gobierno de datos debe considerar usos primarios (el uso para el que los datos fueron recopilados) y secundarios (usos posteriores para otros fines, o usos de datos recopilados por otras dependencias y/o con otros objetivos) de los datos. En particular, el consentimiento informado debe aclarar cuál es el uso que se dará a esos datos y si se van a conservar o van a ser borrados luego del uso.

→

Para seguir leyendo

Para seguir leyendo sobre cómo podemos hacer una gestión de datos eficiente en la Argentina sin poner en riesgo la privacidad, accedé a los documentos de trabajo elaborados por el Área de Datos de Fundar:

Anónimos pero no tanto: cómo hacer una gestión de datos eficiente sin poner en riesgo la privacidad

Datos y algoritmos para el desarrollo

Una propuesta para un sector público basado en datos puede verse aquí:

OECD Working Papers on Public Governance - A data-driven public sector