Protección de datos personales en la Seguridad Social: perspectivas de aplicación de TI

JIAP 2011
Montevideo - URUGUAY

Dr. Ing. Raul Ruggia
Asociación Internacional de Seguridad Social y Universidad de la República

Temario

- **Introducción.**
  - Contexto y definiciones.
  - Protección de Datos Personales.
  - Seguridad Social.
- **Encares basados en TI.**
  - Privacy by Design.
  - Privacy-Enhancing Technologies (PET).
- **Conclusiones.**

Introducción: Contexto (1)

- **Protección de Datos Personales.**
  - Conceptualmente:
    - "*La protección de datos personales es un derecho diferente, pero estrechamente relacionado, con el de la privacidad*". Consejo de Europa.
  - En nuestro contexto lo vemos como:
    - Las reglas que regulan el procesamiento de datos de forma de asegurar el respeto al derecho a la privacidad

Conceptos (1)

- **La normativa Europea define:**
  - *Datos Personales,* como:
    - Toda información sobre una persona física identificada o identificable (el «interesado»);
    - Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente.
  - *Tratamiento de datos personales*, como:
    - Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales,
    - Incluye no solo el relevamiento sino también la conservación de los datos.

Conceptos (2)

- Responsable del tratamiento, como:
  - la persona física o jurídica, … que determine los fines y los medios del tratamiento de datos personales;
- Encargado del tratamiento, como:
  - la persona física o jurídica, …., que trate datos personales por cuenta del responsable del tratamiento;
- Destinatario, como:
  - la persona física o jurídica, …., que reciba comunicación de datos.
- Consentimiento del interesado, como:
  - toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Conceptos (3)

- **Los datos personales deben ser:**
  - Recolectados en forma lícita y con **fines** claramente determinados.
  - Tratados de acuerdo a los fines para los cuales fueron recogidos.
  - Adecuados, pertinentes y **no excesivos** con relación a los fines para los que se recaben.
  - Exactos y, cuando sea necesario, actualizados.
  - Conservados:
    - En una forma que permita la identificación de los interesados.
    - Durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente

Contexto de Seguridad Social (1)

- **Síntesis de Funciones:**
  - Registro / Afiliación de Trabajadores y Empresas.
  - Cálculos de aportes.
  - Recaudación y cobranza de contribuciones.
  - Validación de la elegibilidad.
  - Cálculo de beneficios.
  - Pago de beneficios.
  - Atención al ciudadano.
  - Gestión de reclamos.
  - Análisis de resultados de programas sociales.
  - Análisis de sostenibilidad y prospectiva del sistema.

Contexto de Seguridad Social (2)

- **Operaciones de Seguridad Social.**
  - Uso intensivo de datos de personas y empresas:
    - Datos completos de la persona, de su núcleo familiar, y las actividades laborales incluyendo la remuneración.
    - Datos sobre enfermedades y discapacidades.
    - Aportes realizados y/o adeudados, y multas y sanciones aplicadas.
    - Beneficios recibidos, económicos y no-económicos.
    - Cantidad de empleados y salarios pagados en empresas.
  - Alcanzan un gran porcentaje de la población.
  - Procesamiento de datos intra- e inter-institucion :
    - Empresas, Servicios de Salud, Instituciones de Seguridad Social, prestadores privados de servicios, etc.

Contexto de Seguridad Social (3)

- **Actores**
  - Trabajadores.
  - Empresas.
  - Instituciones (públicas) administradoras de Seg. Social.
  - Instituciones públicas mixtas, que administran programas de Seg. Social y otros (p.ej. Recaudación de impuestos).
  - Instituciones privadas administradoras de programas de Seg. Social (p.ej. Fondos privados (AFAP), mutuales, etc).
  - Instituciones privadas que colaboran en programas de Seg. Social (p.ej. Agentes de pago, bancos, etc).
  - Instituciones públicas no relacionadas con Seg. Social (p.ej. Min. Interior, Educación y Cultura, Economía, etc).
  - Empresas privadas no relacionada con Seg. Social.

Protección de Datos en Seg. Soc.

- **Preguntas que se plantean:**
  - ¿ Qué normas de Protección de Datos Personales son relevantes en operaciones de Seguridad Social ?
  - ¿ Cómo impacta la aplicación de normas de Protección de Datos Personales en Operaciones de Seguridad Social ?
  - ¿ Cómo las TI permiten implementar las operaciones promoviendo la aplicación de las normas ? (respeto por la privacidad)

Protección de Datos en Seg. Soc.

- **Algunos escenarios de interés:**
  - Re-determinación de situación de discapacidad.
  - Proveer información a instituciones comerciales (p.ej. Montos a pagar a través de bancos, etc).
  - Búsqueda e identificación de beneficiarios.
  - Análisis de datos para descubrimientos de fraude.
  - Intercambio de información con otras instituciones/países:
    - Para ejecutar programas sociales.
    - Para realizar estudios estadísticos.

Encares basados en TI

- **Privacy by Design:**
  - Mecanismos para la Protección de Datos previstos desde el diseño de los sistemas.

- **Privacy-Enhancing Technologies (PET).**
  - Conjuntos de medidas basadas en TI para proteger la protección de datos.
  - Evitan procesamiento innecesario y/o no deseado de datos personales.
  - Mantienen las funcionalidades de los sistemas informáticos.

Encare: “Privacy by Design”

- **Mecanismos para Protección de Datos :**
  - Desde el diseño de los sistemas.
  - En lugar de agregarse posteriormente.
- **Un diseñador debe plantearse las preguntas:**
  - ¿ Es necesario recolectar los datos personales ?
  - ¿ Cuáles son los mínimos datos personales a recolectar ?
  - ¿ Quiénes deben tener acceso a qué datos recolectados ?
  - ¿ Cómo controlar el acceso de modo de permitir solo:
    - el relacionado con su propósito ?
    - el acceso de empleados y procesos que lo requieren ?
  - ¿ Cómo apoyar el ejercicio de los derechos de las personas ?

Mecanismos: PET

- **Privacy-Enhancing Technologies (PET).**
  - Mecanismos generales.
    - Encriptación y seguridad en el acceso.
    - Autenticación y autorización de acceso.
    - Control de calidad de datos.
    - Minimización de datos y flujo de datos.
  - Gestión de la Identidad.
  - Seudo-Identidades y Separación de datos.
  - Sistemas de Gestión de Privacidad.
  - Anonimización.
  - Gestión de Consentimiento.
  - Notificaciones a personas.

Mecanismos (1)

- **Minimización de datos.**
  - Eliminar detalles en datos personales que no resultan requeridos.
- **Minimización de flujo de datos:**
  - Flujo de datos estrictamente necesario.
- **Seudo-identidad.**
  - Identificadores generados para el procesamiento de datos personales.
  - Derivables desde los datos de la persona y vice-versa.

Mecanismos (2)

- **Separación de datos**
  - Consiste en generar grupos de datos, separando:
    - Datos que permiten identificar la persona.
      - P.ej. Nombre, dirección, etc.
    - Otros datos.
  - Los grupos de datos se conectan por seudo-identidad.

- **Datos Personales bajo control personal:**
  - Cuando se encuentran en un medio controlado por su propietario:
    - P.ej. Smart cards, dispositivos de almacenamiento personales, Data Safe online.

Mecanismos (3)

- **Componente "*Identity Protector*":**
  - Objetivos:
    - Asegurar que la persona no puede ser identificada a partir de los datos transformados.
    - Asegurar que no pueden obtenerse más datos a partir de datos transformados.
  - Funciones:
    - Genera la seudo-identidades.
    - Separa grupos de datos.
  - Puede consistir en:
    - Funciones especializadas.
    - Sistema de tratamiento de datos personal (p.ej. Smart card).
    - Sistema de tratamiento de datos en institución.

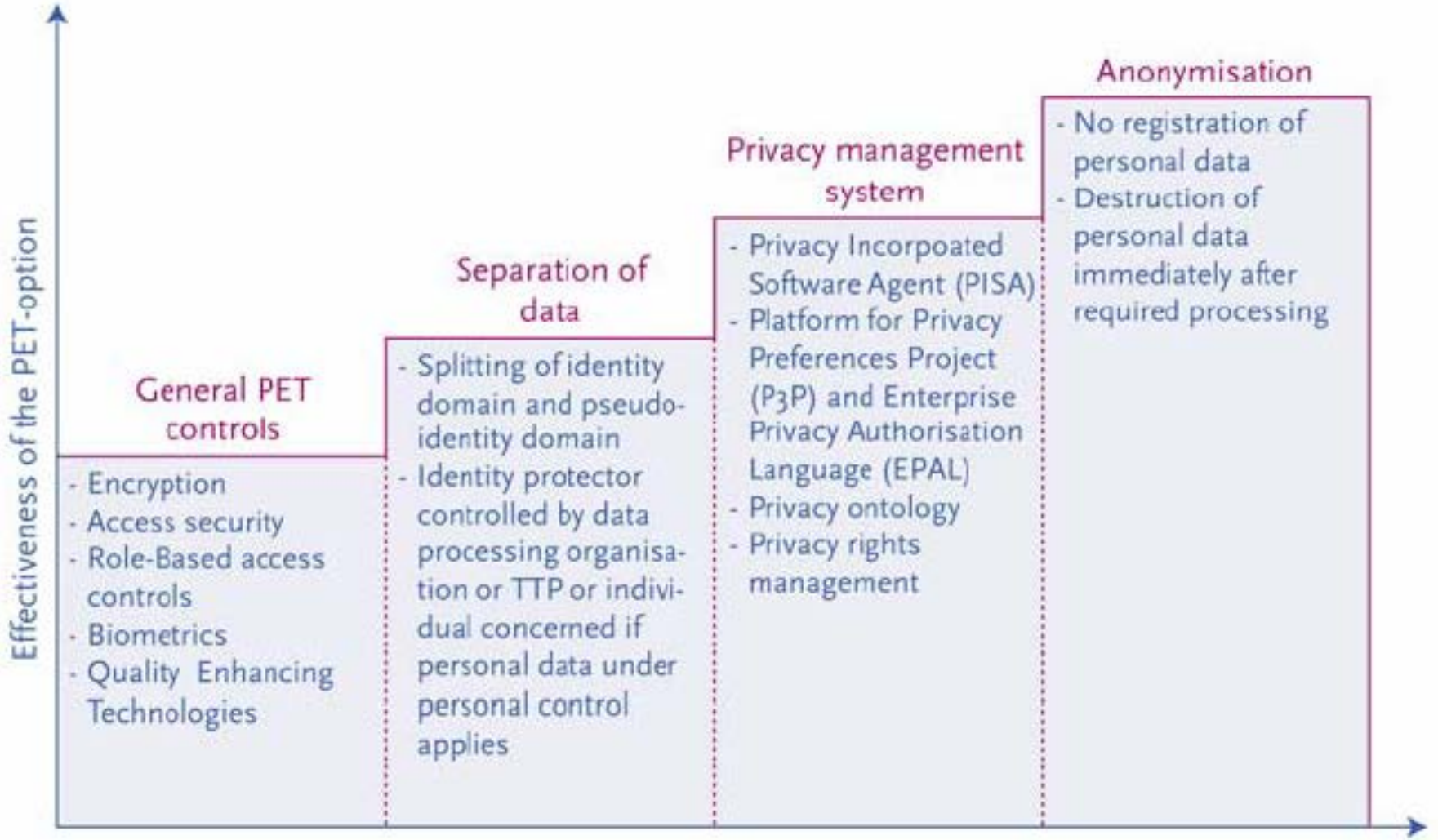
Mecanismos (4)

- **Sistemas de Gestión de Privacidad.**
  - Automatizan el control de las políticas de Prot. Datos.
  - “Recubre” los datos personales y verifica las operaciones que se aplicarán.
    - Basado en “políticas de privacidad” derivadas de normas de protección de datos.
    - Las políticas se especifican a través de Lenguajes de Privacidad.
      - P.ej. EPAL (W3C, OASIS), XACML (OASIS).
  - Han generado resultados interesantes:
    - Incrementan la confianza del público.
    - Automatizan gestión de protección de datos y mejoran su gestión.
      - Reducen complejidad y costos de auditorías.
- **Ejemplo:**
  - Platform for Privacy Preferences Project (P3P) del W3C.

Mecanismos (4)

- **Anonimización.**
  - Consiste en modificar datos personales que sirvan para identificar la persona.
  - Reduce la cantidad de datos a los que se aplican mecanismos de protección.
  - Ejemplos:
    - National Alcohol and Drugs Information System (LADIS) de Holanda, seguimiento a personas con adicciones.
    - Productos de IBM e Infosys.
  - Puede aplicarse en los momentos de:
    - Registro de datos permanente.
    - Recolección de datos temporales.

Mecanismos: Resumen de PETs



[PET – White Paper for Decision Makers, KPMG, 2004]

Otros encares

- **Privacy Impact Assesment (PIA).**
  - Proceso que ayuda a determinar si las tecnologías y sistemas cumplen requerimientos y normas de Privacidad.
  - Se evalúa:
    - Cumplimiento técnico de normativa de Privacidad.
    - Consecuencias más amplias sobre la Privacidad en un sistema.
- **En Plataformas de Gob. Electrónico.**
  - Aprovechamiento de funcionalidades de:
    - Plataforma única para servicios del Estado y Públicos.
    - Seguridad (Identificación, Autenticación y Autorización).
    - Transformación y ruteo centralizado de paquetes de datos (mensajes).

Conclusiones

- **La Protección de Datos Personales:**
  - Constituye una fuerte tendencia en cuanto a prácticas y normativas.
  - Requiere de acuerdos entre instituciones y países.
- **Los sistemas de Seguridad Social:**
  - Hace un uso muy intenso y extenso de datos personales.
  - Presentan operaciones donde debe validarse el cumplimiento de la normativa.
- **Los encares y tecnologías disponibles:**
  - Permiten abordar un conjunto importante de casos.
  - **Se requieren estudios más exhaustivos en países y normativas específicas.**

Muchas gracias