ECIJA GPA
Av. 12 de Octubre N26-97 y Lincoln,
Ed. Torre 1492, 170516. Piso 10 Oficina 1005
Quito - Ecuador
Tel: (+593 2) 2986-528 /29/30
info.ecuador@ecija.com

Biometría y protección de datos personales en el marco de la legislación ecuatoriana

Hoy en día encontramos muchos aplicativos o equipos que utilizan reconocimiento de huella dactilar o facial para permitirnos el acceso a este, pero ¿entendemos lo qué significa dar acceso a ese tipo de datos personales?

Partamos de comprender que la biometría es la identificación de los individuos en función de sus características biológicas o de su comportamiento. La Norma ISO/IEC TR 24741:2018 nos habla de las más frecuentes tecnologías de reconocimiento biométrico y, por poner algunos ejemplos, encontramos: el reconocimiento facial, la huella dactilar, el reconocimiento de voz o iris, la geometría de manos o los datos biométricos de la firma.

Este tipo de datos que recogen una característica física intransferible es en efecto un dato personal al amparo de la Ley Orgánica de Protección de Datos Personales (LOPDP), que incluso lo establece como un dato sensible, con los parámetros que este tipo de datos requiere para su tratamiento.

Ahora, los usos que se le puede dar a estos datos biométricos son variados, pero, a efectos de esta nota, vamos a destacar dos, el primero es la identificación y el segundo es la autenticación o verificación.

Para entender estos usos de mejor manera, me voy a remitir al Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 que recoge las definiciones establecidas por esta entidad, señalando lo siguiente:

> "*Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios)*.
>
> *Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno)*".

De lo expuesto, tenemos que, un ejemplo puede ser el desbloqueo de mi teléfono móvil o celular con reconocimiento facial, estoy realizando un proceso de autenticación o verificación, puesto que previamente ya he cargado esa plantilla en mi equipo y el desbloqueo se produce por el aparejamiento entre esa plantilla y mis datos captados en ese momento.

Por otro lado, cuando a través de una cámara de seguridad que utiliza tecnología de reconocimiento facial se captan mis datos biométricos y se los compara contra una base de datos, estamos hablando de identificación.

Con este antecedente, y para ampliar la visión de estos aspectos en el entorno local, analicemos la reciente Resolución Nro. 003-NG-DINARP-2022 con la que se emite la Norma de Funcionamiento del Sistema de Autenticación Única (SAU). Debo señalar que este análisis no se centra en los aspectos técnicos, al no contar con detalles, solo muestra algunas posibilidades tomadas del marco general del Sistema Nacional de Registros Públicos y, en materia de protección de datos personales, podrían faltar algunos elementos a cumplir respecto de lo establecido en la LOPDP.

En su artículo 5, respecto a la validación de la identidad en el enrolamiento, se incluye como un medio para este fin al reconocimiento facial, el cual se describe en el artículo 16 de la siguiente manera: "*Se validará la identidad del usuario a través del software automatizado de identificación biométrica, capaz de identificar a una persona o de comprobar su identidad mediante la comparación y el análisis de los modelos, formas y proporciones de sus rasgos y contornos faciales*".

En este caso, no podemos hablar de una verificación o autenticación, puesto que al "*validar la identidad*" lo que se pretende es establecer si esa persona es quien dice ser, pero para eso se debe contrastar contra una base de datos de identidad, como la provista por el Registro Civil. Este medio buscaría ser un medio alternativo a la validación que se realiza con el uso del certificado de firma electrónica o ante un fedatario, tal como se ha establecido dentro de la resolución en mención en sus artículos 17 y 18.

Esto deviene de que el SAU busca ser un "*sistema integral de autentificación, autorización y registro único para el acceso seguro a servicios electrónicos gubernamentales integrados para el ciudadano y servidores públicos, a través de un único usuario y contraseña*", de acuerdo al artículo 3 de la mencionada resolución y en ese sentido, los procesos de enrolamiento pretenden que sea solamente el ciudadano solicitante el que pueda habilitarse en este sistema y esto se hace contra la verificación de su identidad en cualquiera de los mecanismos habilitados ya mencionados.

Es decir, que podríamos hablar de un tratamiento con fines de identificación dentro del proceso de enrolamiento a este sistema de autenticación y este debe revestirse del cumplimiento de las condiciones establecidas en la LOPDP, en especial del artículo 26 sobre el tratamiento de datos sensibles, sin dejar de lado el cumplimiento de las demás disposiciones de dicho cuerpo legal.

Así también, es necesario destacar que el uso de datos biométricos es el más intrusivo de los mecanismos planteados en la resolución previamente mencionada ya que, revela más información que un certificado, por ejemplo y entre otros riesgos latentes, a través de su empleo, se puede obtener más información del titular que aquella que este estaría dispuesto a compartir -dependiendo de los datos que se recojan- y este no estaría en capacidad de impedirlo. De esta manera, se debe considerar el impacto que puede tener en los derechos del titular.

Por lo expuesto, al escoger técnicas como esta para el acceso a sistemas como el que se ha planteado, se deben evaluar ciertos aspectos, como por ejemplo, las consecuencias jurídicas de una identificación incorrecta, los criterios a la hora de escoger la tecnología de reconocimiento facial que se utilizará frente al principio de pertinencia y minimización, o la denegación de acceso a servicios causada por errores en la captura o captación del dato.

Área de TMT, Privacidad y Protección de Datos Personales ECIJA Ecuador

info.ecuador@ecija.com

Teléfono: + (593-2) 2986528/29/30/31