**¿Qué consideraciones legales y éticas deben tomarse en cuenta al implementar tecnologías de reconocimiento facial vinculadas a medios de pago, como lo que se está implementando en el sistema público de transporte en Santiago (RED)?**

Para implementar estas tecnologías es fundamental la observancia a lo establecido en la ley 21719 considerando aspectos como:

1. Contar con consentimiento informado de los titulares de los datos (en este caso datos biométricos), además de quienes harán uso de esos datos y los fines específicos, procurando no compartir esos datos con terceros ni para otros objetivos que no sean el de pago en RED, como en este caso.
2. Que los titulares puedan rectificar o eliminar en este caso sus datos en el momento que lo deseen y con las facilidades para ello.
3. Asegurar que las empresas que harán el tratamiento (tanto responsables como madatarios) cumplan a cabalidad con la normativa vigente y con mecanismos de ciberseguridad apropiados para evitar riesgos de usos ilegítimos.

Adicionalmente deben asegurarse aspectos como la no discriminación por género, raza, edad, proporcionar una educación clara a los usuarios para que el consentimiento otorgado sea claro y legitimo.
Como mejores prácticas, las empresas que implementen este sistema deberían realizar un exhaustivo análisis de los riesgos asociados al manejo de este tipo de datos sensibles, detectando de manera preventiva vulnerabilidades y estableciendo claras medidas de protección de los datos tratados, como un cifrado de datos en tránsito y en reposo, realizar supervisiones periódicas del funcionamiento de sus sistemas de ciberseguridad y tener planes de monitoreo continuo.

**¿Qué obligaciones tendrán los operadores tecnológicos, como Evertec, en cuanto a la protección, almacenamiento y uso de datos biométricos en un sistema de pagos como este, una vez que la Ley N° 21.719 y su reglamento se encuentren en plena vigencia?**

Las empresas tecnológicas deben ocuparse de que los responsables de los datos, ya sean las empresas tecnológicas o los clientes de ésta, obtengan el consentimiento explícito de los titulares de los datos, tanto como para almacenamiento como para tratamiento de los mismos. Del mismo modo, garantizar un sistema de revocamiento de esta autorización sencilla, transparente y automática.

Por otra parte, es importante tener en consideración los principios establecidos en la normativa, como por ejemplo que el uso sea exclusivo para la finalidad que han sido otorgados, en este caso en particular, el pago en RED, garantizando su uso exclusivo para este propósito; contar con las medidas de seguridad adecuadas como cifrado, control de acceso, brechas de seguridad, matrices de riesgo, etc.
Las empresas de tecnología deben ocuparse desde el diseño de sus sistemas hasta la implementación, ejecución y mantenimiento de éstos, que se cumplan con las reglas anteriormente descritas. (legalidad, finalidad, proporcionalidad, calidad, seguridad, confidencialidad y protección de los datos).

**¿Cómo se puede garantizar el consentimiento informado de los usuarios en iniciativas voluntarias de este tipo, y qué mecanismos deberán establecerse para revocar dicho consentimiento?**

Se debe asegurar transparencia, seguridad, claridad y facilidad en la gestión de obtención del consentimiento, asi como para su revocación. Para lograr lo anterior, las empresas deben otorgar información clara al titular de los datos sobre la finalidad específica de los datos biométricos entregados, el alcance de este tratamiento, formas de uso y almacenamiento (también cuánto tiempo se mantendrán esos datos en manos de los responsables), los derechos que asisten a los titulares y la identificación de la institución que será responsable de dichos datos ante cualquier vulneración y/o reclamo del titular.
Para garantizar lo anterior, se debe escoger un método explícito mediante la obtención del consentimiento del titular de manera clara y asertiva, como por ejemplo una grabación de voz, marcar una casilla tipo click to accept o algo similar. Para revocar el consentimiento también se debe asegurar una metodología rápiza y fácil, de manera que los usuarios puedan hacer efectiva su decisión de revocación en cualquier momento y de manera inmediata. Los métodos deberían ir en la misma línea que para el otorgamiento, es decir, un botón o número telefónico de fácil acceso y permanentemente a disposición del conocimiento de los usuarios. Las empresas de igual modo deben guardar los registros de revocación, para efectos de responsabilidad y auditorías. El éxito está en disponer canales claros y de fácil acceso para los titulares.

**¿Qué responsabilidades legales podrían derivarse si estos sistemas de reconocimiento facial sufren una filtración o uso indebido de datos ya sea por parte de quien captura la información como de quien la procesa?**

La misma ley establece sanciones fuertes para las brechas de seguridad de los datos personales. Estas sanciones pueden ser económicas, legales y reputacionales, abarcando incluso suspensión de autorizaciones para el tratamiento de datos.
Es importante que las sanciones no sólo pueden recaer en las empresas determinadas como responsables de un eventual incumplimiento, sino que también en las personas detrás de estas, como ejecutivos, directores o funcionarios relacionados.