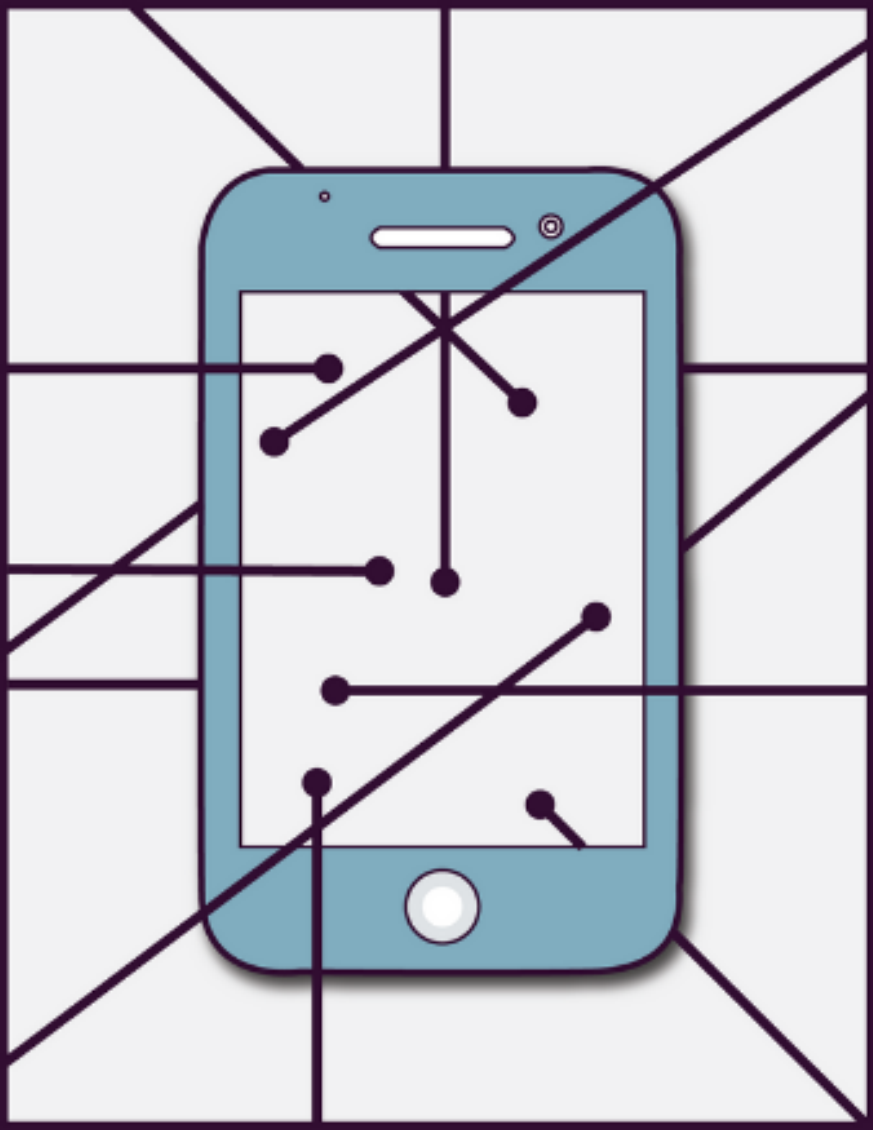
Versión resumida sobre dispositivos electrónicos

Sus derechos de privacidad digital en la frontera



BCCLA

cippic

Versión resumida sobre dispositivos electrónicos

Sus derechos de privacidad digital en la frontera

El objetivo de esta guía es proporcionarle información sobre los derechos de privacidad que tiene con respecto a sus dispositivos electrónicos (como computadoras portátiles, teléfonos celulares y tabletas) al cruzar la frontera. La guía se dirige a personas que cruzan la frontera a Canadá o que viajan a los Estados Unidos a través de los puntos de verificación en origen en Canadá.

Normalmente, la policía no puede hacer revisiones aleatorias sin tener una sospecha, pero la situación en la frontera es diferente. En la frontera se aplica la *Carta Canadiense de Derechos y Libertades*, pero los tribunales han descubierto que, debido a que el gobierno quiere evitar que los bienes peligrosos y las personas no deseables entren al país, la Agencia de Servicios Fronterizos de Canadá (ASFC) tiene más facultad para revisar a las personas y sus posesiones que la policía en otras situaciones.

La *Ley de aduanas* le otorga a la ASFC facultades amplias para revisar a las personas y los bienes que entran al país, incluidas las cosas que la gente trae consigo. Esto incluye el contenido (archivos, fotos y videos) que tiene en sus dispositivos digitales. Conforme a la *Ley de aduanas*, los archivos que tiene en sus dispositivos son "bienes", y los oficiales de aduanas pueden revisar los bienes que entren a Canadá sin una orden, aunque no tengan motivo para sospechar que dichos bienes son o contienen contrabando.

Los no ciudadanos que busquen entrar a Canadá, incluidos los solicitantes de asilo, también pueden ser objeto de revisiones. Conforme a la *Ley de inmigración y protección de refugiados* (IRPA), un oficial de la ASFC puede revisar el equipaje y los efectos personales (incluidos los dispositivos electrónicos y los medios digitales) de una persona que quiere entrar a Canadá a través de un puerto de entrada. Para hacerlo, el oficial tiene que tener:

- Pruebas razonables para pensar que la persona no ha revelado su identidad o que lleva escondidos documentos que son relevantes para su admisibilidad, o
- Pruebas razonables para pensar que la persona está involucrada en tráfico ilegal de personas, trata de personas o fraude documental.

La revisión de dispositivos debe limitarse a identificar a la persona y buscar documentos relevantes para su admisibilidad o pruebas de los delitos que se mencionaron antes.

Revisiones iniciales

Los oficiales de primera línea llevan a cabo revisiones iniciales del contenido de sus dispositivos y verifican las imágenes, los videos y los archivos. Se trata de un examen rápido del contenido para asegurarse de que no sea contrabando (como pornografía infantil o literatura de odio) o pruebas de algún delito. Las revisiones iniciales pueden ser aleatorias o selectivas.

Cualquiera puede ser objeto de una revisión aleatoria. Existe la preocupación de que se seleccione a qué viajeros se va a registrar dependiendo de su raza o religión, y que dicho establecimiento de perfiles pueda hacerse pasar por una revisión "aleatoria". Aunque dicho establecimiento de perfiles sería una violación de la ley, es extremadamente difícil demostrar que se trata de discriminación. Si cree que ha sido objeto de discriminación, a continuación encontrará más información sobre cómo presentar una queja.

En la mayoría de los casos, la ASFC no hace una selección aleatoria de las personas a las que quiere revisar, sino que lo hace de manera selectiva. La selección se basa en información que se encuentra en las bases de datos de viajeros (particularmente para llegadas de vuelos, trenes y cruceros) y en "indicadores"

que, según la Agencia, aumentan la probabilidad de que los dispositivos electrónicos de una persona contengan alguna forma de contrabando. No existe una lista pública de los indicadores que usa la Agencia, pero de manera anecdótica, una persona tiene más probabilidades de que la seleccionen para revisión si:

- Importa algo que la ASFC considera sospechoso, o tiene relación con importadores o exportadores de materiales a los que se opone la Agencia. Esto incluye literatura anime y manga, que la Agencia considera extremadamente sospechosa.
- Ha viajado a destinos "de alto riesgo" (aunque no hay una lista específica, probablemente incluye destinos en el Sudeste de Asia, así como Alemania, Cuba y España).
- Es un hombre soltero que viaja solo.
- Se muestra nerviosa o agitada.
- Lleva consigo varios dispositivos electrónicos (incluidos discos duros).
- Los nombres de los archivos o las carpetas que tiene en su dispositivo demuestran que le interesa la pornografía.
- Compra un boleto para viajar de última hora.
- Su maleta tiene un código que no corresponde con el lugar del que viene.
- Tiene rutas de viaje poco comunes.

Durante la revisión inicial, los oficiales no leen cuidadosamente cada documento ni examinan cada foto que tiene en su dispositivo. Únicamente deben ver el contenido el tiempo necesario para asegurarse de que no se trata de contrabando (como pornografía infantil) o para confirmar o eliminar las sospechas de una violación a la ley de aduanas o migratoria. La información que se encuentre durante una revisión inicial podrá usarse para justificar una revisión más detallada.

Los oficiales únicamente deben ver el contenido que ya se encuentra en su dispositivo. Deben poner el dispositivo en modo de avión y ver únicamente el contenido local (incluidos correos electrónicos y mensajes de texto que se hayan marcado como "leídos"). La ASFC afirma que, para revisar la información a la que sólo se puede acceder de forma remota, debe obtener la orden de un juez. Sin embargo, se sabe de casos en los que la ASFC le ha pedido a un viajero que ingrese de forma voluntaria a una cuenta remota, por lo tanto, los viajeros no pueden estar completamente seguros de que se respetará la privacidad de sus cuentas de redes sociales al cruzar la frontera.

Revisiones detalladas

Si un oficial descubre algo que justifique una inspección más detallada, podrá llevar a cabo una revisión más minuciosa. Los encargados de llevar a cabo estas revisiones minuciosas son especialistas que tienen experiencia en el uso de herramientas forenses.

Para que se lleve a cabo una revisión de este tipo, usted deberá entregar su dispositivo. Conforme a la *Ley de aduanas*, la ASFC está facultada para incautar bienes si un oficial no está convencido de que se verificaron correctamente para ser admitidos a Canadá. Asimismo, los oficiales pueden copiar todo el contenido de su dispositivo. De esa forma, la ASFC puede usar un software de descifrado de contraseñas para obtener acceso al contenido para el que usted no proporcionó una contraseña.

La ASFC asegura que no mantiene copias de los datos una vez que concluye una investigación. Sin embargo, sabemos que la ASFC puede y suele compartir la información personal que reúne con otras dependencias gubernamentales, como la Real Policía Montada de Canadá (RPMC) y otras dependencias

de seguridad como el Servicio de Inteligencia y Seguridad de Canadá (CSIS), quienes a su vez pueden compartirla con gobiernos extranjeros con fines de inteligencia.

Contraseñas

Los oficiales pueden pedirle su contraseña o su huella digital para acceder a la información que tiene almacenada en su dispositivo. No se sabe con certeza si usted tiene la obligación legal de proporcionarles esta información, pero la ASFC ha arrestado o ha amenazado con arrestar a personas que no han querido proporcionar su contraseña. La ASFC afirma que tiene el derecho de arrestar a la gente que no le proporcione su contraseña, y que puede hacerlo cuando un oficial tenga razones para pensar que el dispositivo contiene material prohibido.

La postura de la ASFC en 2017 era que no podía obtener contraseñas a la fuerza para acceder a una cuenta, un archivo o información que esté almacenada de forma remota. Usted no debería enfrentar consecuencia alguna en caso de que se le pida su contraseña para acceder a una cuenta en línea y se niegue a compartirla.

Si se le pide su contraseña y usted decide no divulgarla o no dar su huella digital para acceder a información que está almacenada en su dispositivo, se arriesga a aumentar las sospechas de la ASFC sobre el contenido de su dispositivo, a que se le niegue la entrada al país si no es ciudadano o residente permanente de Canadá, a que se retenga o incaute su dispositivo para que los especialistas forenses lo revisen con más detalle (que podría tomar meses) o a que se le arreste. Entorpecer u obstruir el trabajo de un oficial de la ASFC es un delito que involucra multas de hasta $50,000 y/o cinco años de cárcel.

Áreas de verificación en origen estadounidenses en Canadá

Los oficiales del Servicio de Aduanas y Protección Fronteriza de los Estados Unidos tienen autorización para aplicar las leyes estadounidenses en las partes de los aeropuertos, terminales ferroviarias y terminales de transbordadores canadienses en las que las personas que viajan a los Estados Unidos pueden pasar por la aduana estadounidense antes de salir de Canadá. En estas áreas, la aplicación de las leyes estadounidenses está sujeta a las leyes canadienses sobre derechos humanos, incluida la *Carta Canadiense de Derechos y Libertades*. En otras palabras, se aplican las normas de registro e incautación canadienses y no las estadounidenses. No obstante, no es claro si los oficiales fronterizos estadounidenses tienen conocimiento de las normas legales adecuadas ni se sabe si están capacitados para aplicarlas.

Las leyes estadounidenses relativas a la revisión de dispositivos electrónicos son similares a las canadienses: los oficiales no necesitan una orden ni sospecha razonable para revisar su teléfono. Esto se limita únicamente al contenido local y no abarca información para la que sea necesario tener una conexión a la red.

Los oficiales fronterizos estadounidenses llevan a cabo revisiones básicas y avanzadas. Las revisiones básicas pueden efectuarse aunque no se tengan sospechas e implican revisar un dispositivo electrónico con menos detenimiento que una revisión avanzada.

En la revisión avanzada, el dispositivo se conecta a un equipo externo para obtener acceso a su contenido, pero también con la posible intención de copiarlo. Para que se lleve a cabo una revisión, se necesita una sospecha razonable de violación a las leyes estadounidenses o una preocupación sobre la seguridad nacional.

Los oficiales fronterizos estadounidenses pueden pedirle su contraseña. Si usted se niega a compartirla, el oficial podrá negarle la autorización previa para que pueda viajar a los Estados Unidos. Asimismo, podrá retener su dispositivo para poder efectuar una revisión más detallada. Aunque no deben retener su dispositivo por más de cinco días, se han reportado casos en de dispositivos que han retenido durante varios meses.

Consejos

Cuando piense qué medidas puede tomar para proteger su privacidad, debe estar consciente de que el tono de su interacción con un oficial fronterizo puede intensificarse si este descubre que usted trató deliberadamente de impedir una revisión, especialmente de alguna forma que destruya los datos a los que habría tenido acceso, o si descubre que escondió el hecho de que existen esos datos.

- **Deje sus dispositivos en casa** si no los necesitará durante su viaje o **use un dispositivo especial para viajar** que no contenga datos ni actividad.
- **Saque un respaldo** de sus datos antes de cruzar la frontera y déjelo en casa. Esto es importante por si se retiene o incauta su dispositivo, pero también porque le permite borrar datos innecesarios de su dispositivo antes de cruzar la frontera. También le recomendamos eliminar todo el contenido de su dispositivo antes de cruzar la frontera y restablecerlo posteriormente a partir de su respaldo.
- **Elimine de forma segura los datos** que no necesitará durante su viaje. Esto no significa simplemente dejarlo en la papelera de reciclaje, sino usar las herramientas incluidas en Windows (una herramienta que se llama *cipher*), Mac (*vaciar la papelera de forma segura* o *srm*) o Linux (*shred* o *srm*) para eliminar los datos permanentemente. Recuerde de que las agencias fronterizas tienen acceso a herramientas forenses sofisticadas y pueden ver información sobre los datos eliminados que la mayoría de la gente no puede ver. Presionar en el botón “eliminar” no garantiza que un oficial fronterizo no podrá encontrar la información.
- **Establezca una contraseña** para entrar o acceder a su dispositivo. Puede ser que, por curiosidad, un oficial encienda su dispositivo electrónico para ver el contenido y pierda el interés cuando se dé cuenta de que tiene que pedirle su contraseña.
- **Cree una contraseña segura**, por ejemplo, use varias palabras aleatorias (una “frase de contraseña”), de ser posible, y evite contraseñas que se puedan adivinar fácilmente.
- **Apague su computadora** antes de pasar por la aduana y asegúrese de que sus cuentas o aplicaciones no estén configuradas para que pueda ingresar a ellas automáticamente cuando se activen.
- **Use la autenticación de dos factores**, por si el oficial fronterizo incauta un dispositivo y no el otro.
- **Use el cifrado de disco completo** y establezca una frase de contraseña sólida para acceder a él. Muchos dispositivos nuevos ya incluyen esta opción, que le permite mantener sus datos seguros y fuera del alcance de los analistas más experimentados. Sin embargo, no se sabe con certeza qué sucederá si se retiene su dispositivo electrónico y los oficiales fronterizos no pueden acceder a sus datos. Puede ser que incauten su dispositivo y no se lo devuelvan.
- Si decide no usar el cifrado de disco completo, puede **cifrar ciertos documentos o archivos críticos** usando el software incluido en su dispositivo.
- **Guarde los documentos privilegiados y confidenciales** en una carpeta por separado para que quede claro que son privilegiados. Algunos ejemplos de estos archivos son los de abogados o, a

veces, de médicos, psicólogos o psiquiatras o periodistas. Se supone que los oficiales fronterizos deben tomar precauciones para no ver material privilegiado cuando se les advierte que existe, salvo que sea para verificar que realmente se trata del material que usted declaró. En teoría, no deben ver los archivos privilegiados, pero puede ser que no respeten la ley en estas situaciones.

Cómo presentar una queja

Si cree que su revisión no fue apropiada, pero su queja no es sobre discriminación ni invasión de privacidad, puede presentarla ante la Agencia de Servicios Fronterizos de Canadá. Si se incautó su dispositivo, o si recibió una sanción o una multa, puede solicitar una revisión de la decisión.

También puede mandar sus comentarios al Recourse Directorate (Dirección de Recursos) de la ASFC, que revisará la conducta del oficial. Asegúrese de incluir toda la información relevante para que el oficial de recursos entienda su queja y pueda responderle.

Si cree que ha sido víctima de discriminación por parte de un oficial de la ASFC, puede presentar una queja ante la Canadian Human Rights Commission (Comisión Canadiense de Derechos Humanos). Puede ser víctima de discriminación por raza, origen nacional o étnico, color, religión, edad, género, orientación sexual, identidad o expresión de género, estado civil, estado familiar, discapacidad, características genéticas o una condena para la que se ha concedido indulto o cuyo registro ha quedado suspendido.

Si siente que la ASFC invadió su privacidad, puede presentar una queja ante la Office of the Privacy Commissioner of Canada (Oficina del Comisionado Privado de Canadá), que vigila que el gobierno cumpla con la Ley de privacidad.

Asimismo, puede reportar los incidentes relevantes a los grupos de derechos civiles correspondientes de Canadá, como el International Civil Liberties Monitoring Group (Grupo Internacional de Vigilancia de las Libertades Civiles) y/o el National Council of Canadian Muslims (Consejo Internacional de Musulmanes Canadienses).

Si cree que se ha violado su privacidad o que ha sido víctima de discriminación por parte de los oficiales estadounidenses en las áreas de verificación en origen, le recomendamos que escriba al Minister of Public Safety (Ministro de Seguridad Pública) y al Minister of Foreign Affairs (Ministro de Asuntos Exteriores). También puede comunicarse con la Office for Civil Rights and Civil Liberties (Oficina de Derechos y Libertades Civiles del Departamento de Seguridad del Territorio Nacional, el Chief Privacy Officer (Director responsable de la protección de la intimidad) del Departamento de Seguridad del Territorio Nacional y el Traveler Redress Inquiry Program (Programa de Consultas de Desagravio de Pasajeros) del Departamento de Seguridad del Territorio Nacional. También puede reportar los incidentes relevantes a los grupos de derechos civiles correspondientes, como la Electronic Frontier Foundation, el Council on American-Islamic Relations (Consejo de Relaciones Estadounidenses-Islámicas) y la American Civil Liberties Union (Unión Americana de Libertades Civiles).

www.bccla.org

@bccla

@BCCivLib

www.cippic.ca

@cippic

This project was supported by a grant from the Canadian Internet Registration Authority's (CIRA) Community Investment Program.