Un jurado de la corte federal de Estados Unidos encontró al ex director de seguridad de Uber, Joseph Sullivan, culpable de no revelar una violación de los registros de clientes y conductores en 2016 a los reguladores, además de intentar encubrir el incidente.

Sullivan ha sido condenado por dos cargos: uno por obstruir la justicia al no denunciar el incidente y otro por cometer errores. Enfrenta un máximo de cinco años de prisión por el cargo de obstrucción y un máximo de tres años por el segundo.

> *«Las empresas de tecnología en el Distrito Norte de California recopilan y almacenan grandes cantidades de datos de los usuarios»*, dijo la fiscal federal Stephanie M. Hinds, en un comunicado de prensa.

> *«Esperamos que esas empresas protejan esos datos y alerten a los clientes y a las autoridades competentes cuando los hackers roben dichos datos. Sullivan trabajó afirmativamente para ocultar la violación de datos de la Comisión Federal de Comercio y tomó medidas para evitar que los hackers fueran atrapados».*

El hackeo de Uber en 2016 ocurrió como resultado de dos hackers que obtuvieron acceso no autorizado a las copias de seguridad de la base de datos de la compañía, lo que llevó a la empresa de transporte compartido a pagar en secreto un rescate de 100 mil dólares en diciembre de 2016, a cambio de eliminar la información robada.

Uber también hizo que los extorsionadores firmaran un acuerdo de confidencialidad en un intento de hacer pasar el robo como una recompensa por errores. Las copias de seguridad contenían datos pertenecientes a 50 millones de usuarios de Uber y 7 millones de conductores.

Para complicar más las cosas, el incidente ocurrió cuando el Departamento de Justicia de Estados Unidos y la Comisión Federal de Comercio (FTC) ya estaban investigando a la

empresa por otra violación de datos que ocurrió el 13 de mayo de 2014.

En febrero de 2015, Uber reveló que se había accedido de forma indebida a una de sus bases de datos después de un posible compromiso de una de las claves de cifrado, lo que resultó en la exposición de nombres y números de licencia de aproximadamente 50,000 conductores. El incidente fue descubierto el 14 de septiembre de 2016.

> *«Después de engañar a los consumidores sobre sus prácticas de privacidad y seguridad, Uber agravó su conducta indebida al no informar a la Comisión que sufrió otra filtración de datos en 2016 mientras la Comisión investigaba la filtración sorprendentemente similar de la empresa en 2014»,* dijo la FTC en 2018.

El Departamento de Justicia dijo que Sullivan desempeñó un papel crucial en la configuración de la respuesta de Uber a la FTC con respecto a la violación de 2014, y el acusado testificó bajo juramento el 4 de noviembre de 2016 sobre la cantidad de pasos que afirmó que la empresa había tomado para proteger los datos de los usuarios.

Los fiscales federales también acusaron a Sullivan de mentirle al director ejecutivo de Uber, Dara Khosrowshani, así como a los abogados externos de la compañía que investigaban el incidente de 2016, afirmando que *«la verdad sobre la violación»* finalmente salió a la luz en noviembre de 2017.

Además, se dice que Travis Kalanick, cofundador y luego director ejecutivo de Uber, quien renunció a la compañía en junio de 2017, aprobó la estrategia de Sullivan para manejar la intrusión no autorizada. Kalanick no ha sido acusado.

En un comunicado compartido con The New York Times, el equipo legal de Sullivan dijo que su úico enfoque durante el transcurso del incidente y su carrera profesional ha sido garantizar la *«seguridad de los datos personales de las personas en Internet».*

El desarrollo, que marca la primera vez que un alto ejecutivo de la compañía enfrenta cargos

penales por una violación de datos, se produce cuando los dos hackers involucrados en el incidente de 2016 esperan sentencia por sus cargos de conspiración de fraude después de declararse culpables del delito en octubre de 2019.

> *«Las declaraciones de culpabilidad separadas presentadas por los hackers demuestran que después de que Sullivan ayudó a encubrir el hackeo de Uber, los hackers pudieron cometer una intrusión adicional en otra entidad corporativa, Lynda.com, e intentar rescatar esos datos también»,* dijo el Departamento de Justicia.

A pesar de que las fallas de seguridad de 2014 y 2016 se reflejaron entre sí, Uber fue el centro de atención el mes pasado por razones equivocadas cuando sus sistemas fueron violados por tercera vez en un ataque que desde entonces, ha vinculado al grupo de hackers LAPSUS$.

En julio pasado, Uber también llegó a un acuerdo con el Departamento de Justicia para pagar 148 millones de dólares y acordó *«implementar un programa de integridad corporativo, salvaguardas específicas de seguridad de datos y planes de notificación de violación de datos y respuesta a incidentes, junto con evaluaciones bienales».*

> *«El mensaje del veredicto de culpabilidad de hoy es claro: las empresas que almacenan los datos de sus clientes tienen la responsabilidad de proteger esos datos y hacer lo correcto cuando se producen infecciones»,* dijo el agente especial a cargo del FBI en San Francisco, Robert K. Tripp.