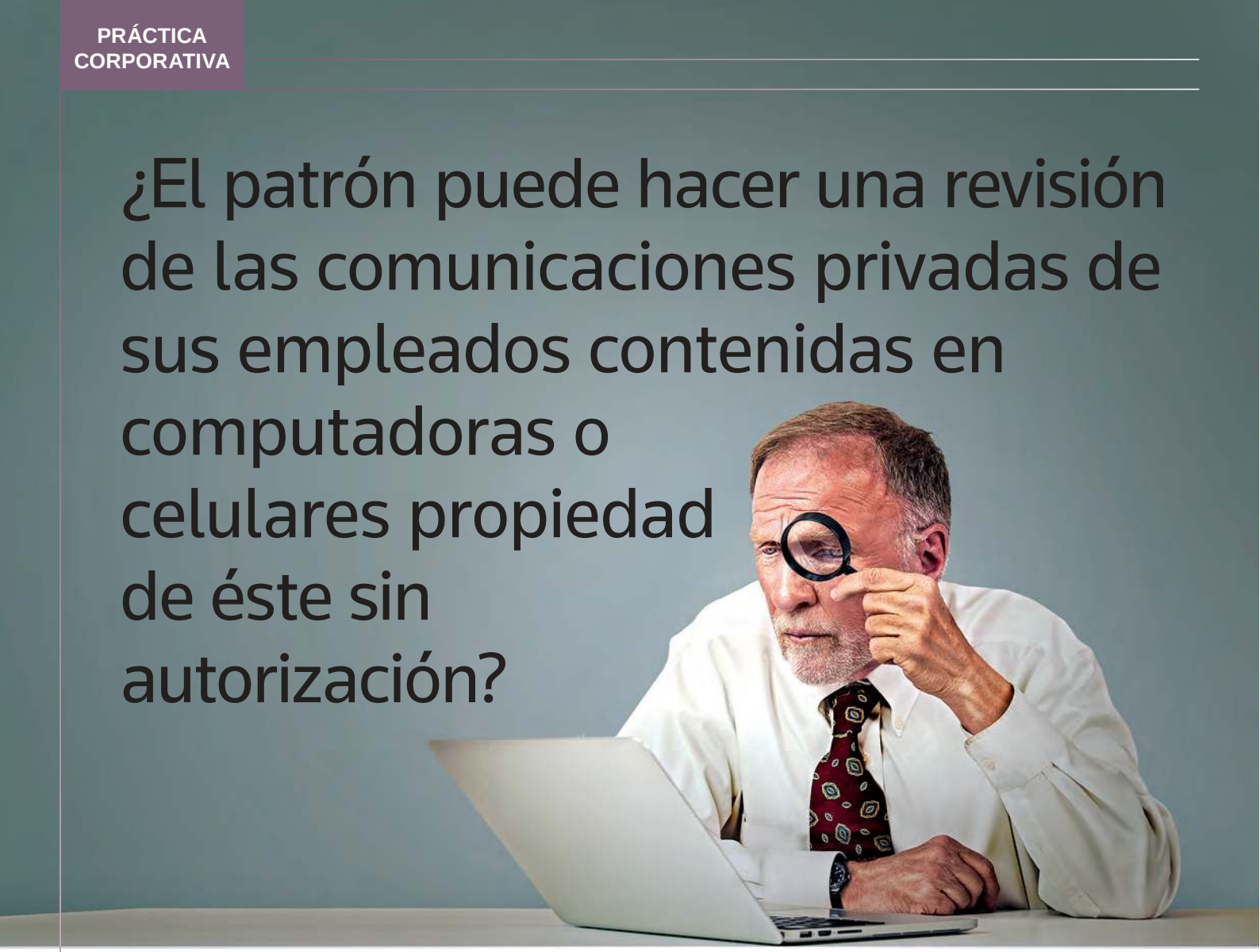
¿El patrón puede hacer una revisión de las comunicaciones privadas de sus empleados contenidas en computadoras o celulares propiedad de éste sin autorización?



La cultura de la legalidad y el cumplimento regulatorio en esta época están exigiendo que cada empresa mantenga el debido control organizacional, conforme a la naturaleza de sus actividades y operación, para el logro de su legítimo objeto social. En ese sentido, lo primero que debe entenderse es que para atribuir responsabilidad penal a la persona jurídica, en su caso, se parte siempre de una persona física quien ha cometido un hecho delictivo. En ese contexto, habrá que darle la bienvenida a la era del *compliance penal* en la cual se integran, en forma interdisciplinaria, materias como gobierno y Derecho Corporativo, protección de datos personales, políticas anticorrupción, Derecho Laboral, Derecho Informático y Derecho Penal, entre otras

Autor: Carlos Requena, Socio
de Requena Abogados

INTRODUCCIÓN

Las corporaciones y organizaciones en México están obligadas a adaptarse a la era del *compliance penal*, toda vez que, como personas morales o jurídicas, serán responsables penalmente cuando las personas sometidas a la autoridad de sus representantes y/o administradores, realicen un delito "por no haberse ejercido sobre ellas el debido control que corresponda al ámbito organizacional que deba atenderse según las circunstancias del caso", y la conducta delictiva se realice con motivo de actividades sociales, por cuenta, provecho o exclusivo beneficio de la corporación.[1]

ESTADO DE LA CUESTIÓN

En esta era de constante y abundante regulación de las actividades comerciales de las empresas, los dueños y administradores enfrentan la necesidad de verificar que sus empresas y empleados se integren a la cultura de la legalidad y el cumplimento regulatorio.

Es en este sentido que surge la necesidad y justificación de que cada empresa mantenga el debido control organizacional, conforme a la naturaleza de sus actividades y operación, para logro de su legítimo objeto social.

Por consiguiente, las empresas en México deberán abandonar el aparente cumplimiento regulatorio, *compliance* o autorregulación, ése que les sirve sólo como mera "fachada cosmética", con la intención de erigirse como supuestas "empresas socialmente responsables", pero sin una real vocación de legalidad.

Es decir, ahora sí les llegó el momento de enfrentar el desafío de desarrollar una verdadera cultura empresarial de autorregulación en materia de prevención delictiva, condicionada a su propia dimensión corporativa.

Al respecto, resulta indudable que un sano gobierno corporativo, la implementación de las mejores prácticas corporativas y la adopción de modelos eficaces de gestión empresariales, permitirán generar una **cultura de cumplimiento**, complementada con reglas y códigos de conducta para ejercer la administración y el control de las empresas, alcanzando el **equilibrio adecuado entre la capacidad empresarial y el manejo de los recursos humanos y económicos**. El fin último es lograr un sano beneficio al interior, y generar un valor compartido al exterior con el entorno.

CONTEXTO LEGAL Y NORMATIVO

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece, entre otras cuestiones, que:

> ...
> *Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*

Asimismo, la CPEUM también señala que:

> ...
> *Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.*

En consecuencia –a manera de primera conclusión–, se afirma que las comunicaciones privadas son inviolables y exclusivamente la autoridad judicial federal podrá autorizar la intervención de cualquier comunicación privada.

Sin embargo, para contextualizar el tema de las *responsabilidades penales*, es necesario transcribir algunas tesis emitidas por la Suprema Corte de Justicia de la Nación (SCJN) relacionadas con la comisión de un ilícito constitucional.

> ***COMUNICACIONES PRIVADAS. EL DERECHO A SU INVIOLABILIDAD, CONSAGRADO EN EL ARTÍCULO 16, PÁRRAFO NOVENO, DE LA CONSTITUCIÓN FEDERAL, ES OPONIBLE TANTO A LAS AUTORIDADES COMO A LOS GOBERNADOS, QUIENES AL TRANSGREDIR ESTA PRERROGATIVA INCURREN EN LA COMISIÓN DE UN ILÍCITO CONSTITUCIONAL.*** *Del análisis de lo dispuesto en diversos preceptos de la Constitución Política de los Estados Unidos Mexicanos, se advierte que la misma contiene mandatos cuyos destinatarios no son las autoridades, sino que* ***establece deberes a cargo de los gobernados****, como sucede, entre otros casos, de lo dispuesto en sus artículos 2o., 4o. y 27, en los que la prohibición de la esclavitud, el deber de los padres de preservar el derecho de los menores a la satisfacción de sus necesidades y a la salud física y mental, así como los límites a la propiedad privada, constituyen actos u omisiones que deben observar aquéllos, con independencia de que el mandato constitucional constituya*

[1] Código Penal para el Distrito Federal, **Responsabilidad Penal de las Personas Morales o Jurídicas**, artículo 27 y siguientes

una garantía exigible a las autoridades y que, por ende, dentro de su marco competencial éstas se encuentren vinculadas a su acatamiento. En tal virtud, al establecer el Poder Revisor de la Constitución, en el párrafo noveno del artículo 16 de la Constitución General de la República, que las "comunicaciones privadas son inviolables", resulta inconcuso que ***con ello estableció como derecho fundamental el que ni la autoridad ni los gobernados pueden intervenir una comunicación****, salvo en los casos y con las condiciones que respecto a las autoridades establece el propio numeral y, por tanto,* ***la infracción de los gobernados a tal deber conlleva la comisión de un ilícito constitucional****, con independencia de los efectos que provoque o del medio de defensa que se prevea para su resarcimiento, en términos de la legislación ordinaria correspondiente.*

Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

No. de Registro 190652. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XII. Segunda Sala. Materia constitucional. Tesis aislada. Tesis 2a. CLX/2000. Diciembre, 2000. Pág. 428.

(Énfasis añadido.)

COMUNICACIONES PRIVADAS. LAS PRUEBAS OFRECIDAS DENTRO DE UN JUICIO CIVIL, OBTENIDAS POR UN GOBERNADO SIN RESPETAR LA INVIOLABILIDAD DE AQUÉLLAS, CONSTITUYEN UN ILÍCITO CONSTITUCIONAL, POR LO QUE RESULTAN CONTRARIAS A DERECHO Y NO DEBEN ADMITIRSE POR EL JUZGADOR CORRESPONDIENTE. *El artículo 16, párrafo noveno, de la Constitución Política de los Estados Unidos Mexicanos establece que las comunicaciones privadas son inviolables; que exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada; que dicha petición deberá ser por escrito, en la que se funden y motiven las causas legales de la solicitud, expresando el tipo de intervención, los sujetos de la misma y su duración; y que no se podrán otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. El párrafo décimo de dicho numeral señala que las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes, y que los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio. Ante ello, debe estimarse que fue voluntad del Poder Revisor de la Constitución establecer como derecho fundamental la inviolabilidad de las comunicaciones privadas y, en contrapartida, la obligación exigible tanto a las autoridades como a los gobernados de respetar dicha prerrogativa, lo que da lugar a que* ***si un gobernado realiza la intervención de alguna comunicación privada sin el consentimiento expreso e irrefutable de los que la entablan, incurrirá en un ilícito constitucional****; por ende, si dentro de un juicio civil, en cualquiera de sus especies, una de las partes ofrece como prueba la grabación de* ***una comunicación privada que no fue obtenida legalmente, tal probanza debe estimarse contraria a derecho*** *y, por tanto, no debe admitirse por el juzgador correspondiente, pues ello implicaría convalidar un hecho que en sí mismo es ilícito.*

Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

No. de Registro 190651. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XII. Segunda Sala. Materia constitucional. Tesis aislada. Tesis 2a. CLXI/2000. Diciembre, 2000. Pág. 428.

(Énfasis añadido.)

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MOMENTO EN EL CUAL SE CONSIDERA INTERCEPTADO UN CORREO ELECTRÓNICO. El correo electrónico se ha asemejado al correo postal*, para efectos de su regulación y protección en el ordenamiento jurídico. Sin embargo, es necesario identificar sus peculiaridades a fin de estar en condiciones de determinar cuándo se produce una violación a una comunicación privada entablada por este medio. A los efectos que nos ocupan,* ***el correo electrónico se configura como un sistema de comunicación electrónica virtual, en la que el mensaje en cuestión se envía a un "servidor"****, que se encarga de "enrutar" o guardar los códigos respectivos, para que el usuario los lea cuando utilice su operador de cuenta o correo. La utilización del correo electrónico se encuentra supeditada a una serie de pasos determinados por cada servidor comercial. Así, es necesario acceder a la página general del servidor en cuestión, donde se radican todos los mensajes de la cuenta de correo contratada por el titular. Esta página suele estar compuesta por dos elementos:* ***el nombre de usuario (dirección de correo electrónico del usuario o*** **login***) y la contraseña (*password***). De vital importancia resulta la contraseña, ya que ésta es la llave personal con la que cuenta el usuario para impedir que terceros puedan identificarla y acceder a la cuenta personal del usuario****. La existencia de esa*

clave personal de seguridad que tiene todo correo electrónico, ***lo reviste de un contenido privado y por lo tanto investido de todas las garantías derivadas de la protección de las comunicaciones privadas y la intimidad. En esta lógica, se entenderá que un correo electrónico ha sido interceptado cuando –sin autorización judicial o del titular de la cuenta– se ha violado el*** **password** ***o clave de seguridad****. Es en ese momento, y sin necesidad de analizar el contenido de los correos electrónicos, cuando se consuma la violación al derecho fundamental a la inviolabilidad de las comunicaciones privadas. No sobra señalar, que si bien es cierto que un individuo puede autorizar a otras personas para acceder a su cuenta –a través del otorgamiento de la respectiva clave de seguridad– dicha autorización es revocable en cualquier momento y no requiere formalidad alguna. Asimismo,* ***salvo prueba en contrario, toda comunicación siempre es privada****, salvo que uno de los intervinientes advierta lo contrario, o bien, cuando de las circunstancias que rodean a la comunicación no quepa duda sobre el carácter público de aquélla.*

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

No. de Registro 161339. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XXXIV. Primera Sala. Materia constitucional. Tesis aislada. Tesis 1a. CLIX/2011. Agosto, 2011. Pág. 218.

(Énfasis añadido.)

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. IRRELEVANCIA DE LA PROPIEDAD DE LA COMPUTADORA PARA EFECTOS DE CONSIDERAR INTERCEPTADO UN CORREO ELECTRÓNICO. *Para efectos de la protección constitucional del derecho fundamental a la inviolabilidad de las comunicaciones privadas,* ***no es posible afirmar que alguien se encuentra legitimado para interceptar el correo electrónico de un tercero, al ser de su propiedad la computadora desde la que se accedió a la cuenta de correos. Esto es así, ya que una de las principales características del correo electrónico es su virtualidad y su ubicuidad, en tanto que se puede acceder a él desde cualquier computadora conectada a la red. En esta lógica, lo relevante para efectos de su protección constitucional, es el proceso comunicativo en sí mismo, con independencia del tipo de computadora a través de la cual se acceda a la cuenta o de quién sea el propietario del ordenador, cuestiones meramente accidentales.***

Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

No. de Registro 161341. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XXXIV. Primera Sala. Materia constitucional. Tesis aislada. Tesis 1a. CLX/2011. Agosto, 2011. Pág. 217.

(Énfasis añadido.)

Respecto a la protección de las comunicaciones privadas, la Primera Sala de la SCJN resolvió la siguiente tesis:

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO TEMPORAL DE PROTECCIÓN. *La inviolabilidad de las comunicaciones privadas, en lo que respecta a su ámbito temporal de protección, se extiende también con posterioridad al momento en el que se produce la comunicación. Esto resulta de especial importancia en aquellos casos en los que el mensaje se materializa en un objeto una vez finalizado el proceso comunicativo, ya que existen muchos medios de comunicación que, por su naturaleza, conservan el contenido de las conversaciones.* ***Así, el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, no sólo proscribe aquellas interceptaciones de comunicaciones en tiempo real –es decir, durante el tiempo en que efectivamente se entabla la conversación–, sino también aquellas injerencias que se realizan con posterioridad en los soportes materiales que almacenan la comunicación.***

Amparo directo en revisión 1621/2010.15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

No. de Registro 161336. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XXXIV. Primera Sala. Materia constitucional. Tesis aislada. Tesis 1a. CLVI/2011. Agosto, 2011. Pág. 220.

(Énfasis añadido.)

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASE-

GURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO. *En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que* ***todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica deben protegerse por el derecho fundamental a su inviolabilidad, como sucede con el teléfono móvil en el que se guarda información clasificada como privada*** *por la Primera Sala de la Suprema Corte de Justicia de la Nación; de ahí que el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo,* ***ya sea en forma de texto, audio, imagen o video****. Por lo anterior, no existe razón para restringir ese derecho a cualquier persona por la sola circunstancia de haber sido detenida y estar sujeta a investigación por la posible comisión de un delito, de manera que si la autoridad encargada de la investigación, al detenerla, advierte que trae consigo un teléfono móvil, está facultada para decretar su aseguramiento y solicitar a la autoridad judicial la intervención de las comunicaciones privadas conforme al citado artículo 16 constitucional; sin embargo,* ***si se realiza esa actividad sin autorización judicial, cualquier prueba que se extraiga, o bien, la que derive de ésta, será considerada como ilícita y no tendrá valor jurídico alguno***

Contradicción de tesis 194/2012, entre las sustentadas por el Segundo Tribunal Colegiado en Materias Penal y Administrativa del Décimo Séptimo Circuito y el Cuarto Tribunal Colegiado del Décimo Octavo Circuito. 10 de octubre de 2012. La votación se dividió en dos partes: mayoría de cuatro votos por lo que se refiere a la competencia. Disidente: José Ramón Cossío Díaz. Unanimidad de cinco votos en cuanto al fondo. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Jorge Antonio Medina Gaona. Tesis de jurisprudencia 115/2012 (10a.). Aprobada por la Primera Sala de este Alto Tribunal, en sesión de fecha diecisiete de octubre de dos mil doce.

No. de Registro 2002741. Semanario Judicial de la Federación y su Gaceta. Décima Época. Libro XVII. Tomo I. Primera Sala. Materia constitucional. Tesis de jurisprudencia. Tesis 1a./J. 115/2012 (10a.). Febrero, 2013. Pág. 431.

(Énfasis añadido.)

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A TELÉFONOS O APARATOS DE COMUNICACIÓN ABANDONADOS O RESPECTO DE LOS CUALES NO SE TENGA CONOCIMIENTO DE QUIÉN ES SU TITULAR, POR LO QUE PARA ACCEDER A SU INFORMACIÓN DEBE SOLICITARSE LA AUTORIZACIÓN DE UN JUZGADOR FEDERAL. *Esta Primera Sala de la Suprema Corte de Justicia de la Nación ha sostenido que* ***todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben protegerse por el derecho fundamental a la inviolabilidad de las comunicaciones privadas****; así, lo que está prohibido por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos* ***es la intercepción o el conocimiento antijurídico de una comunicación ajena realizada por particulares o por alguna autoridad****. Ahora bien,* ***la violación del derecho referido se consuma en el momento en que se escucha, graba, almacena, lee o registra –sin el consentimiento de los interlocutores– una comunicación ajena****, con independencia de que con posterioridad se difunda el contenido de la conversación interceptada. En estas condiciones, para que sea constitucional la intervención de cualquier comunicación privada, en términos del referido artículo, deberá existir, indefectiblemente, control judicial previo por parte de un juzgador integrante del Poder Judicial de la Federación. Consecuentemente, al poseer el derecho a la inviolabilidad de las comunicaciones privadas, autonomía propia y al configurar una garantía formal que protege las comunicaciones con independencia de su contenido, éste se extiende a teléfonos o aparatos de comunicaciones abandonados o respecto de los cuales no se tenga conocimiento de quién es su titular, por lo que la autoridad competente deberá solicitar la autorización de un juzgador federal para acceder a la información contenida en un aparato de comunicación en dichos supuestos. Lo anterior se justifica, porque la única excepción para que no exista control judicial previo para intervenir algún tipo de comunicación*

privada, es que ***alguno de los participantes en la comunicación aporte la información a las autoridades competentes voluntariamente.***

Amparo directo en revisión 3506/2014. 3 de junio de 2015. Cinco votos de los Ministros Arturo Zaldívar Lelo de Larrea, José Ramón Cossío Díaz, Jorge Mario Pardo Rebolledo, Olga Sánchez Cordero de García Villegas y Alfredo Gutiérrez Ortiz Mena. Los Ministros Zaldívar, Pardo, Sánchez Cordero y Gutiérrez, reservaron su derecho para formular voto concurrente. Ponente: José Ramón Cossío Díaz. Secretaria: Rosalba Rodríguez Mireles. Esta tesis se publicó el viernes 28 de agosto de 2015 a las 10:30 horas en el Semanario Judicial de la Federación.

No. de Registro 2009820. Gaceta del Semanario Judicial de la Federación. Décima Época. Libro 21. Tomo I. Materia constitucional. Primera Sala. Tesis aislada. Tesis 1a. CCLIII/2015 (10a.). Agosto, 2015. Pág. 465.

(Énfasis añadido.)

Por su parte, a nivel de la legislación federal, el Código Penal Federal (CPF) dispone en los artículos 177, 211 BIS, 211 BIS-1 (párrafo 2), lo siguiente:[2]

> ***Artículo 177.*** *A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*
>
> ***Artículo 211 BIS.*** *A quien revele, divulgue o utilice* ***indebidamente o en perjuicio de otro****, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*
>
> ***Artículo 211 BIS-1.*** *...*
>
> *Al que* ***sin autorización*** *conozca o copie información* ***contenida en sistemas o equipos de informática*** *protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*
>
> *(Énfasis añadido.)*

INVITACIÓN AL DEBATE JURÍDICO

Asumamos, para los efectos del presente análisis, que la empresa no tuvo el debido cuidado, desde el inicio de la relación laboral entre este patrón y el empleado, de documentar la previa autorización –del trabajador– para efectuar cualquier tipo de revisión o auditoría futura a la computadora, correo electrónico y/o celular durante el tiempo en que se mantenga la relación laboral, precisamente respecto de estos equipos o dispositivos tecnológicos

[2] El énfasis es nuestro

suministrados por el patrón al trabajador para el exclusivo desarrollo de sus actividades laborales en favor de la empresa o del legítimo cumplimiento del objeto social corporativo.

Es evidente que el contenido de tal computadora, correos electrónicos y celular constituyen comunicaciones privadas, pero lo importante en esta discusión, materia del tema que nos ocupa, estriba en determinar si ese ámbito de protección constitucional también actualiza a "la contraseña" o "*password* de seguridad" con el que dicho empleado cuenta para el acceso a esa computadora, correos electrónicos y celular, propiedad del patrón. Es decir, si es posible homologar tal contraseña o *password,* también como una comunicación privada.

Ahora bien, para efectos penales y la determinación de una probable conducta delictiva, es necesario analizar el elemento de la "probable ilicitud", consistente en que la intervención a tales comunicaciones privadas se haga *sin autorización*, a fin de responder a la pregunta inicial de la presente discusión:

¿Viola un patrón las comunicaciones privadas de sus empleados, contenidas en computadoras o celulares propiedad del patrón, al hacerles una revisión o auditoría, sin la previa autorización del empleado?

Contextualizando la respuesta al caso aquí asumido, frente a una interpretación armónica y teleológica de las disposiciones constitucionales, legales y criterios judiciales, considero válido proponer una segunda conclusión, en el sentido de que no habrá ninguna violación por parte del patrón en agravio de su trabajador, si el patrón dispone de contratos laborales con cláusulas expresas de previa autorización de sus empleados para efectuar cualquier revisión o supervisión a los contenidos de las comunicaciones de los dispositivos tecnológicos, propiedad del patrón, pero dados en tenencia a los empleados con motivo de la relación laboral y durante el tiempo que dure ésta.

Sin embargo, insisto en que no toda empresa o patrón cuenta con esa autorización formal y previa de sus empleados, situación que obliga a esos patrones y a sus administradores a formular algunas preguntas, las cuales transcribiré y trataré de responder para determinar si se actualiza la violación ilícita a comunicaciones privadas y, en consecuencia, la comisión de un probable ilícito penal atribuible al patrón.

¿Existe algún impedimento legal para revisar el contenido de un equipo de trabajo, específicamente una computadora laptop, suministrada a un empleado para el cumplimiento de sus actividades laborales en la empresa, a pesar de no existir el consentimiento expreso y previo de ese empleado o revisarla en su ausencia?

Respuesta: No existe impedimento legal alguno, siempre y cuando esa revisión la haga el patrón, por medio de sus representantes, apoderados o encargados de las áreas de auditoría interna, conforme al legítimo ejercicio de los principios y normas que rigen en el Derecho Laboral, y con base en la relación de subordinación laboral empleado-patrón.

En efecto, el artículo 134 de la Ley Federal del Trabajo (LFT) dispone que son *obligaciones* de los trabajadores:

> ...
> ***I.*** *Cumplir las disposiciones de las normas de trabajo que les sean aplicables;*
> ...
> ***III.*** *Desempeñar el servicio bajo la dirección del patrón o de su representante, a cuya autoridad estarán subordinados en todo lo concerniente al trabajo;*
> ***IV.*** *Ejecutar el trabajo con la intensidad, cuidado y esmero apropiados y en la forma, tiempo y lugar convenidos;*
> ...
> ***VII.*** *Observar buenas costumbres durante el servicio;*
> ...

Adicionalmente, existe un imperativo categórico establecido en el artículo 135 de la LFT, al ordenar que *queda prohibido* a los trabajadores:

> ...
> ***IX.*** *Usar los útiles y herramientas suministrados por el patrón, para objeto distinto de aquél a que están destinados; y*
> ...

La respuesta a esta pregunta tiene como base el análisis e interpretación de las disposiciones de orden público en materia de Derecho Laboral como causa de justificación en favor del patrón que elimina toda ilicitud penal que pudiera atribuirse a éste.

Asimismo, la interpretación legal de los artículos citados de la LFT pudiera eventualmente complementarse con cualquier política interna, código de ética laboral y/o manifestación que haya mediado entre el patrón y los empleados durante el tiempo de duración de la relación laboral.

Un aspecto importante es acreditar, por cualquier medio lícito, que tal computadora o celular, los usa el empleado como útiles o herramientas suministradas por el patrón, pero quedando claro, exteriorizado y evidente *el conocimiento del empleado* de que deberá destinarlos al objeto de sus actividades laborales.

Al monitorear el equipo de trabajo de los empleados, específicamente una computadora o laptop suministrada a ese trabajador para el cumplimiento de sus activi-

dades laborales, ¿se estaría vulnerando el derecho a la inviolabilidad de las comunicaciones privadas establecido en la Constitución Federal?

Respuesta: No, siempre y cuando quede plenamente comprobado que el equipo revisado o monitoreado le fue suministrado al empleado para la realización de sus actividades relacionadas precisamente con su labor, y que ese trabajador recibió tal equipo (computadora o celular) bajo el conocimiento de que debe destinarlos a ese objetivo del trabajo.

Es decir, siempre y cuando se demuestre que el empleado exteriorizó su conocimiento de que recibía la posesión o tenencia de tal equipo de cómputo –o celular– para el cumplimiento de sus actividades laborales. Máxime que también seguramente se acreditará que tales equipos o dispositivos tecnológicos son propiedad del patrón o que esta empresa tiene la legítima disposición sobre ellos por virtud, ejemplo, de un contrato de arrendamiento.

¿La empresa, sus representantes, funcionarios y/o empleados estarían corriendo algún riesgo de responsabilidad penal por realizar la revisión o auditoría periódica de los equipos de trabajo proporcionados a los trabajadores para desempeño de su labor?

Para efecto de dar respuesta, debe recordarse que las comunicaciones privadas son inviolables, como derecho fundamental y, de manera general, la autoridad o los gobernados no pueden intervenir una comunicación privada, salvo en los casos y con las condiciones que la ley autoriza.

En principio, toda comunicación privada que es ofrecida como prueba en un procedimiento penal y no fue obtenida legalmente, debe estimarse contraria a derecho y, por tanto, no debe admitirse por la autoridad correspondiente, pues ello implicaría convalidar un hecho que en sí mismo es ilícito. Sin embargo, lo relevante es definir qué son o qué se entiende por **comunicaciones privadas en el contexto de una relación laboral.**

Entonces, en ese orden de ideas, el correo electrónico se ha asemejado al correo postal ordinario para efecto de su regulación y protección en el ordenamiento jurídico. Al respecto, es necesario identificar sus peculiaridades, para estar en condiciones de determinar cuándo se produce una violación a una comunicación privada emanada por este medio electrónico.

El correo electrónico se configura como un sistema de comunicación electrónica virtual, en la que el mensaje en cuestión se envía tecnológicamente a un "servidor", que se encarga de "enrutar" o guardar los códigos respectivos, para que el usuario los lea cuando utilice su operador de cuenta o correo.[3]

La utilización del correo electrónico se encuentra supeditada a una serie de pasos determinados por cada "servidor privado para efecto comercial". En este sentido, es necesario acceder a la página general del servidor en cuestión, donde radican todos los mensajes de la cuenta de correo contratada "por el titular", en este caso, la empresa o patrón, propietaria del servidor utilizado para el cumplimiento de sus actividades y objeto social. Esta página o plataforma electrónica suele estar compuesta por dos elementos: **(i)** El nombre de usuario, dirección de correo electrónico del usuario o *login,* y **(ii) La contraseña, clave de acceso o *password***.

De vital importancia resulta la naturaleza y alcances de la contraseña o *password*, pues ésta es la llave personal a la que tiene acceso el usuario, en este caso el empleado, para impedir que ***terceros*** puedan invadirla y acceder indebidamente a la cuenta personal del usuario-empleado que se le asignó para el cumplimiento de sus actividades laborales.

Es decir, considero que esa contraseña o *password* no es propiedad del trabajador, sino del patrón quien le permite usar como protección contra terceros ajenos a la relación laboral. Tal contraseña está destinada a impedir que ***terceros a la relación laboral***, entre dicho empleado y el patrón, accedan indebida o ilícitamente a la información o comunicación privada.

Por tanto, la existencia de esa contraseña, *password* o clave personal de seguridad que tiene todo correo electrónico, lo reviste de un contenido privado, por lo cual se encuentra investido de todas las garantías derivadas de la protección de las comunicaciones privadas y la intimidad.

En esta lógica, como regla general se entenderá que un correo electrónico ha sido interceptado ilícitamente cuando sin autorización judicial o sin la autorización del titular de la cuenta, se ha violado tal *password* o clave de seguridad.

Por otra parte, para efectos de la protección legal del derecho fundamental a la inviolabilidad de las comunicaciones privadas, no es posible afirmar que alguien se encuentra legitimado para interceptar o intervenir el correo electrónico de un "tercero", a pesar de ser de su propiedad la computadora desde la que se accedió a la cuenta de correo.

Una de las principales características del correo electrónico es su virtualidad y su ubicuidad, en tanto que se puede acceder a él desde cualquier computadora conectada a la red. En este sentido, lo relevante para efectos de su protección legal es el proceso comunicativo en sí mismo, con independencia del tipo de computadora a través de la cual se acceda a la cuenta o de quién sea el propietario del "ordenador", como cuestiones meramente accidentales.

[3] Nava Garcés, Alberto Enrique. *La prueba electrónica en materia penal.* Editorial Porrúa, México, 2011

Ahora toca dar respuesta a la pregunta encomendada, siendo importante distinguir las afirmaciones anteriores, y que han sido corroboradas por algunos Tribunales federales mexicanos, pues una cosa es la irrelevancia de la propiedad de la computadora *(hardware)* y otra, la importancia de la contraseña *(password)* que se le autoriza al empleado a crear para seguridad contra terceros –ajenos a la relación laboral–, al momento de asignarle la computadora propiedad del patrón, suministrada para la realización de sus actividades laborales como empleado.

Si bien la contraseña o *password* es de vital importancia por ser la llave personal con la que cuenta el usuario (empleado) para impedir que **terceros** puedan identificarla y acceder, siendo esa contraseña personal de seguridad la llave de acceso al correo electrónico y, por tanto, contraseña considerada como contenido privado investida de las garantías derivadas de la protección de las comunicaciones privadas y de la intimidad, también lo es que **la empresa o patrón no es un tercero** en y frente al sistema integral de comunicaciones que genera el usuario-empleado para el ejercicio de sus funciones laborales.

Precisamente por este motivo, el artículo 135, fracción IX de la LFT, disposición de orden público e irrenunciable, establece a los empleados la obligación de usar el equipo, útiles y herramientas de trabajo **exclusivamente para las actividades relacionadas con sus funciones laborales; actividades de las cuales no puede ser ajeno ni tercero el propio patrón.**

Interpretar que los trabajadores de una empresa pueden "tener, generar o crear" una llave, clave de acceso, contraseña o *password* en forma total y exclusivamente privada, con el fin de imposibilitar a su patrón el revisar, monitorear o auditar sus actividades o el contenido de sus comunicaciones realizadas, recibidas o transmitidas en su carácter de empleado en los equipos de cómputo que precisamente se le suministraron –incluido el correo institucional corporativo– sería absurdo e iría en contra de los principios de subordinación, deber de obediencia laboral, lealtad, transparencia, control y supervisión con motivo de la relación de trabajo patrón-empleado.

Asimismo, y precisamente con base en la relación laboral patrón-empleado, y habiendo tenido conocimiento el empleado de que su patrón le concedió el equipo de cómputo, incluido el correo electrónico el cual está enlazado a un "dominio" y "servidor" propiedad del patrón, es evidente que el legítimo ejercicio de control, revisión y supervisión de las actividades laborales, por parte del patrón o empresa, no puede conllevar la intervención ilícita de comunicación privada, materia de los correos electrónicos generados por el empelado del sistema informático, dominio o servidor propiedad del patrón.

Esta legitimidad de patrón para revisar, monitorear o auditar el contenido de las computadoras institucionales, correos electrónicos y celulares de la empresa, suministrados a los empleados, incluyen todo tipo de contenido, es decir, incluso el que aparentemente y de primera intención parecería exclusivo del empleado, incluso, como ejemplo, en el caso del uso de correos electrónicos vía *Gmail*, *Hotmail* u otros, dejados en bandejas, carpetas o archivos electrónicos de la computadora suministrada al empleado.

Por consiguiente, toda comunicación que pasa, se transfiere, almacena, guarda, circula o borra de los instrumentos, herramientas o dispositivos electrónicos, en el contexto de la relación laboral, pueden legítimamente ser revisados, monitoreados o auditados por los patrones o empresa, al tener causa de justificación laboral suficiente, situación que imposibilita se les atribuya una violación ilícita de comunicaciones privadas.

En efecto, pues nótese que no se está alterando, encriptando y ni siquiera haciendo actividad engañosa con la contraseña o *password* generado por el trabajador.[4] Insisto en que el patrón tiene en todo momento el derecho de supervisión, control y revisión de todo el contenido de información almacenada o transmitida en sus computadoras, dispositivos tecnológicos, servidores, correos electrónicos y sistemas informáticos en general, pues –en mi consideración– tal empresa o patrón **no es un tercero ajeno** a la legitimidad del acceso o conocimiento del contenido de tales comunicaciones privadas en el contexto de la relación laboral frente al usuario-empleado, en el contexto del cumplimiento del objeto social o actividades relacionadas con las labores del trabajador.

Lo importante es que toda supervisión, control, monitoreo y/o revisión de comunicaciones privadas generadas por los empleados en ese contexto de su relación de subordinación laboral, puede dar como resultado la legítima extracción de tales comunicaciones, conforme a los principios y justificación del Derecho Laboral, códigos de ética, procesos y/o las políticas internas de la empresa, para ser consideradas como lícitas y, en su caso, tener valor probatorio en cualquier procedimiento legal.

Si se pretendiera acusar penalmente al patrón y/o sus representantes de una extracción ilícita de la información generada por el empleado, recordemos que el CPF[5] establece como causas de exclusión del delito, en su artículo 15, entre otras, en la fracción II, que el delito se excluye cuando se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito que se trate de imputar, en este caso, la inexistencia del dolo por parte del patrón, sus administradores, revisores o auditores.

Incluso, la fracción VI del citado artículo dispone que el delito se excluye cuando la acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, *siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro.*

En una revisión, monitoreo o auditoría el patrón no actúa con dolo, sino en cumplimiento de su rol de patrón frente a la relación de subordinación laboral para control y supervisión de las actividades laborales de sus empleados, como parte de su control organizacional corporativo.

Concretamente en la Ciudad de México, las corporaciones y organizaciones están obligadas a ejercer sobre sus administradores y empleados, "el debido control que corresponda al ámbito organizacional que deba atenderse según las circunstancias del caso" e, incluso, "a establecer medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo el amparo de la persona moral o jurídica".[6]

Si existe algún impedimento legal, ¿qué consecuencias jurídicas para la empresa y para los empleados se generan por realizar las actividades de revisión, monitoreo o auditoría?

Respuesta: En caso de que no haya legítima justificación conforme al Derecho Laboral, no haya existido autorización alguna bajo la relación de subordinación laboral, no exista conocimiento del empleado de que los equipos se le suministraron para sus actividades laborales y/o se haya violado, alterado, manipulado o realizado actividad engañosa sobre la contraseña personal, clave de acceso o *password* generado por el usuario-empleado, eventualmente pudieran ser imputados de un delito penal los administradores o representantes del patrón que hayan actuado dolosamente para la extracción ilícita de información o comunicación privada con el solo propósito de perjudicar al empleado injustificadamente.

¿Existe alguna consecuencia penal o impedimento en realizar esta función de revisión, monitoreo o auditoría en horario no laboral ordinario, en ausencia del trabajador, y sin su conocimiento y sin su previa autorización expresa?

[4] Insisto en que la contraseña, llave de seguridad o *password* no es propiedad del empleado, sino que es generado por él y le es permitido su uso, pero para proteger de intervenciones o intrusiones contra terceros ajenos a la relación laboral

[5] Todos los Códigos Penales establecen causas de exclusión del delito. Ejemplo: en el Distrito Federal el artículo 29, fracción IV (Ejercicio de un derecho) dispone que cuando el agente realice una acción o una omisión atendiendo a su derecho, siempre que exista necesidad racional de la conducta empleada para ejercerlo

[6] Artículos 27 BIS. (Responsabilidad penal de una persona moral o jurídica) y 27 QUINTUS, del Código Penal para el Distrito Federal (CPDF)

Respuesta: El monitoreo, como se ha expresado, es lícito conforme a las disposiciones y principios del Derecho Laboral.

Lo delicado puede surgir si el Ministerio Público investigador, ante una denuncia penal formulada por algún empleado o ex empleado, cuestiona que dicha revisión, monitoreo o auditoría se haya realizado en horario "no laboral" respecto del horario de los monitores, auditores o supervisores. Es decir, distinguiendo entre el horario laboral propio del empleado-monitoreado y el horario de los auditores-monitores. Asimismo, pudiera cuestionarse, de ser el caso, que se abrió la puerta de alguna oficina exclusivamente destinada al empleado-monitoreado cuya computadora se revisó, estando dicha puerta cerrada y la computadora adentro de su oficina.

En ese sentido, también se debería revisar la política interna aplicable, pues una cosa es acceder legítimamente a la computadora y correos electrónicos, y otra, ingresar a una oficina cerrada en horario no laboral del empleado-monitoreado. Esto último debería estar también protegido y amparado por la relación propia del Derecho Laboral, conforme a las políticas de seguridad internas.

En otras palabras, se debe justificar la "versión legitimadora" de los hechos, del porqué se monitoreó el equipo en esa forma, lugar, tiempo y modo específicos, a fin de estar en posibilidad de demostrar que el patrón, por conducto de los auditores-monitores, ejerció derechos laborales y cumplió con las políticas internas, como causa de justificación excluyente de cualquier delito.

¿Se puede emplear la información obtenida mediante esta función de monitoreo o auditoría como medio de prueba dentro de un procedimiento jurisdiccional de naturaleza penal?

Respuesta: Sí, en principio.

El Ministerio Público investigador requerirá que el patrón, por conducto de sus representantes, demuestre el tiempo, lugar, modo y circunstancia específica en que la evidencia, datos, información, peritajes y/o pruebas, fueron descubiertos, encontrados, conocidos, extraídos y/o documentados, a fin de dar credibilidad y legitimidad a la denominada "cadena de custodia" y al origen lícito de los datos de prueba para efectos de su validez procesal.

Así, para tal efecto, el Ministerio Público tiene facultades de investigación para citar a declarar a todos y cada una de las personas relacionadas con la auditoría o monitoreo o, en su caso, para ordenar la práctica de las "entrevistas", por medio de la policía de investigación, a cualquier persona interviniente o posible testigo de los hechos.

Asimismo, asumiendo que no se haya violado, alterado, manipulado ni engañado lo relativo al *password* generado por el empleado, sino que el patrón, por conducto de sus representantes, obtuvo la información usando legítimamente los códigos de acceso propios de la empresa para acceder o revisar los sistemas de cómputo, el servidor y/o una computadora en concreto, físicamente o en forma remota, deberá documentar y justificar el procedimiento y tal uso de las Tecnologías de la Información y Comunicación (TIC) dentro del contexto de la relación laboral.

¿Las respuestas anteriores cambiarían en el supuesto de que los trabajadores proporcionaran su autorización expresa previo al control de vigilancia, monitoreo o auditoría?

Respuesta: Sí. Cualquier autorización oral o expresa del empleado, previa o indirecta, por medio de la cual exteriorice su aceptación y/o conocimiento de las políticas internas o códigos de ética o procedimientos de control y auditoría, que se pueda legítimamente demostrar ante las autoridades, anula o excluye la posibilidad de la comisión de algún delito imputable al patrón.

En caso de que lo anterior no sea suficiente, ¿pueden proponernos algún mecanismo que elimine riesgos legales al revisar, monitorear o auditar periódicamente los equipos de trabajo y que haga que la información obtenida sea admisible en procedimientos penales?

Respuesta: Sí.

Se recomienda documentar por medio de algún formato escrito, adiciones al contrato laboral o al momento de la concreción e inicio de la relación de trabajo, el señalamiento expreso de la facultad de supervisión, control, monitoreo y revisión por parte del patrón, de todos los equipos de trabajo suministrados al trabajador, incluyendo cualquier contenido o comunicación que se encontrare o haya transmitido en éstos, respecto de los cuales los empleados reconocen y dan su consentimiento de que cualquier contraseña, clave de acceso o *password* que llegaren a crear, usar o generar con motivo del uso y la prestación de sus servicios laborales, no es impedimento para que el patrón ejercite tales facultades, en cualquier tiempo, modo, lugar y circunstancia como parte de la política de debido control organizacional de empresa. Asimismo, reconociendo que dicha contraseña, clave de acceso o *password* tiene como finalidad proteger la información contra terceros ajenos a la estricta relación laboral.

CONCLUSIONES

Las comunicaciones privadas, contenidas en útiles, herramientas, instrumentos o dispositivos electrónicos (computadoras, correos electrónicos y/o celulares) de los empleados, pueden ser legítimamente intervenidas, revisadas, auditadas o monitoreadas por el patrón, por conducto de sus representantes, siempre y cuando justifiquen tal actuación en el contexto y al amparo de una legítima relación laboral, y que tales equipos sean propiedad del patrón.

El imperativo categórico establecido en el artículo 135 de la LFT, al ordenar que *queda prohibido* a los trabajadores usar los útiles y herramientas suministrados por el patrón, para objeto distinto de aquél al que están destinados, debe interpretarse sistemática y teleológicamente con las demás disposiciones y principios del Derecho Laboral, Derecho Constitucional y criterios de los Tribunales federales, en el sentido de que el patrón tiene en todo momento el derecho de supervisión, control, auditoría y revisión del contenido, comunicaciones e información almacenada en las computadoras, dispositivos tecnológicos, servidores, correos electrónicos y/o sistemas informáticos en general, propiedad del patrón, pues –en mi opinión– tal empresa o patrón **no es un tercero ajeno** a la relación laboral.

Por tanto, el patrón tiene la legitimidad del acceso o conocimiento del contenido de tales comunicaciones privadas, incluso por encima de la contraseña, clave de seguridad o *password* que genera el trabajador, siempre y cuando todo se realice en el contexto de la relación laboral, durante el tiempo en que ésta dure y con el conocimiento del empleado de que debe destinar el uso de tales equipos al cumplimiento legítimo del objeto social de la empresa.

Concretamente en la Ciudad de México, conforme a la legislación relacionada con la responsabilidad penal de las empresas, las corporaciones y organizaciones están obligadas a ejercer sobre sus administradores y empleados el debido control que corresponda al ámbito organizacional que deba atenderse según las circunstancias del caso e, incluso, a establecer medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo el amparo de la persona moral o jurídica.

En consecuencia, una buena práctica corporativa es reconocer el derecho de los patrones o empresas a ejercer mecanismos de supervisión, monitoreo, control y revisión de todo el contenido e información almacenados o transmitidos en o desde las computadoras, dispositivos tecnológicos, servidores, correos electrónicos y sistema informático en general, propiedad de las empresas.

Coincido con la sugerencia y necesidad de que las empresas cuenten con una previa, debida y bien desarrollada política de protección de datos[7] y manejo de información para que, desde el inicio de las relaciones de trabajo entre el patrón y los empleados, éstos otorguen su consentimiento previo autorizando a que durante el tiempo en que dure la relación laboral, se pueda realizar cualquier legítima revisión o auditoría a los medios de comunicación, propiedad de la empresa, suministrados a los trabajadores para el cumplimiento de sus actividades laborales.

En caso de que no se cuente con ese previo consentimiento o autorización por parte de los empleados, considero que subsiste el derecho de los patrones para supervisión, control, auditoría y monitoreo a sistemas de información, siempre y cuando no se altere, destruya ni engañe la contraseña, llave de seguridad o *password* que es generado por el trabajador, sin ser de su propiedad.

Es decir, siempre y cuando se utilicen los códigos de acceso generales de seguridad del patrón, pues tal contraseña o *password* se crea para evitar que terceros, ajenos a la relación de trabajo, puedan intervenir ilícitamente las comunicaciones privadas dentro del contexto laboral.

Bienvenida la era del *compliance penal* donde se integran, en forma interdisciplinaria, materias como: Gobierno y Derecho Corporativo; Protección de datos personales; Políticas anticorrupción; Derecho Laboral; Derecho Informático, y Derecho Penal, entre otras.

La cultura de legalidad corporativa tiende a evitar o reducir considerablemente los riesgos, y un buen gobierno corporativo integra reglas y conductas para ejercer la administración, el control y la operación de las empresas, cuyo objetivo es establecer el equilibrio entre la capacidad empresarial y el debido control organizacional, así como entre el desempeño laboral y el cumplimiento regulatorio.

Nuestra actual sociedad de riesgos o de la inseguridad conduce necesariamente a las políticas de vigilancia y prevención empresariales, ante los mercados altamente complejos, competitivos y con estructuras donde las personas físicas pueden aprovechar para generar ambientes criminógenos.

La mejor estructura corporativa no garantizará los resultados ni el rendimiento, pero la estructura corporativa equivocada es una garantía de fracaso.
Peter Drucker

Carlos Requena
Socio de Requena Abogados

[7] Revista Abogado Corporativo, Septiembre-Octubre 2015, Práctica Corporativa, pág. 64, artículo de Carlos Vital Román Sánchez, Director Jurídico de PricewaterhouseCoopers, S.C