Internet y Privacidad en las Empresas: entre Políticas, Delitos y Garantías Constitucionales en Argentina.

Marcelo G. I. Temperini

Estudiante de Derecho de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral. Analista de Seguridad y Vulnerabilidad en Redes (ESR), certificado por Cisco. Socio Fundador de AsegurarTe, una Consultora en Seguridad Informática.
mtemperini@asegurarte.com.ar

Abstract. La potestad de control de monitoreo y acceso por parte del empleador a las comunicaciones electrónicas de sus empleados, debe ser ejercido de manera informada, consentida y razonable. En el ámbito laboral, los límites a la privacidad de los dependientes por parte del principal se vuelven difusos, generando inseguridad jurídica en las empresas, dada sus consecuencias graves en responsabilidad civil y penal. Son las políticas de privacidad un documento necesario para determinar el correcto uso de los recursos corporativos de la empresa u organización, entre ellos, la utilización del correo electrónico. A través de la teoría de control restringido se propone delimitar con precisión aquellos casos en donde el empleador podría utilizar el nivel más intrusivo de control, el acceso a los contenidos de las comunicaciones electrónicas. Redacción, documentación, consentimiento, proporcionalidad y motivación son los elementos fundamentales de una adecuada política de privacidad.

Introducción.

Un nuevo mundo se está dibujando para nuestra generación y sin duda el protagonista de los cambios tecnológicos más radicales es Internet. En esta red de redes de enorme potencial, en donde es posible realizar una innumerable cantidad de actividades. En un mundo virtual donde la información se transmite en todo momento, sin demoras y sin intermediarios.

La revolución tecnológica más importante del último siglo ha venido de la mano de la llamada nueva era de la información, en la cual la posesión del poder ya no depende de tener más propiedades, más riquezas, ni más ejércitos o tropas militares como en otros tiempos. Hoy, el poder de los nuevos personajes se mide en niveles de información.

Pensando en este contexto, se plantea como objetivo poder mostrar la realidad del derecho de privacidad en las empresas y sus implicancias en la potestad de control del empleador.

Fuentes normativas.

El art. 18 de nuestra Constitución Nacional determina que el domicilio es inviolable como también la correspondencia epistolar y los papeles privados. Resulta así concordante con el texto del art. 19, donde es claro que el legislador ha pretendido mantener una gama del obrar humano alejado del contralor o la intromisión del Estado.

La prescripción del art. 19 de nuestra norma fundamental, expresa la base misma de la libertad moderna, donde "la convicción según la cual es exigencia elemental de la ética que los actos dignos de mérito se realicen en virtud de la libre creencia del sujeto en los valores que los determinan."[1]

La intromisión con repercusión en dichas dimensiones sólo podrá justificarse sobre la base de casos excepcionales y extremos.

A partir de la reforma de 1994, con la incorporación de los Tratados Internacionales, entre ellos, en la Convención Interamericana de Derechos Humanos, podemos encontrar 2 artículos claves que ayudan a nuestra tarea de delimitación de fuentes del derecho de privacidad. En el art. 11 en particular el inc. 2 que afirma *"Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación."* y el inc. 3 *"Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*.

En el ámbito nacional, la normativa de fondo ha previsto el carácter de ilícito civil a aquellos actos que arbitrariamente impliquen la intromisión en la vida ajena, contemplado esto en el art. 1071 bis del Código Civil.

Otras leyes, guardan entre sus artículos, diferentes grados de protección del derecho de privacidad, así como la Ley 11.723, en su art. 31, protegiendo así el derecho a la imagen de las personas, como de los aspectos de importancia de la privacidad.

En la Ley 19.728, podemos encontrar también una norma que resguarda el derecho a la privacidad de las personas, más precisamente en el art. 18: *"La correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente"*.

A partir de la reforma constitucional del año 1994, se ha incorporado en el art. 43 de nuestra constitución el derecho de Habeas Data, que en el año 2000 dió lugar a la Ley 25.326 de Protección de Datos Personales, cuyo objeto, enunciado en el artículo 1ro, es la *"protección de los datos personales... para garantizar el derecho al honor y la intimidad de las personas, así como también el acceso a la información..."*.

Así, podemos mencionar otras normas que tienen por objeto la protección de este derecho fundamental de las personas, pero es suficiente a modo breve de repaso.

Jurisprudencia de la Corte Suprema.

El 24 de Febrero de 2009, se ha pronunciado la resolución que ha traído un interesante debate relativo a nuestra materia. El fallo caratulado como "Halabi,

[1] Fernández, Claudio: http://www.delitosinformaticos.com/ciberderechos/privacidad.shtml

Ernesto c/ P.E.N. ley 25.873 dto. 1563/04 s/ amparo ley 16.986", ha tenido como eje de debate una acción de amparo accionada por el actor reclamando la inconstitucionalidad de la ley 25.873 y de su decreto reglamentario, por considerar que sus disposiciones vulneran las garantías establecidas en los artículos 18 y 19 de la Constitución Nacional, en cuanto autorizan la intervención de las comunicaciones telefónicas y por Internet sin que una ley determine en qué casos y con qué justificativos. Alegó que esa intromisión constituye una violación de sus derechos a la privacidad y a la intimidad en su condición de usuario, a la par que menoscaba el privilegio de confidencialidad que, como abogado, ostenta en las comunicaciones con sus clientes.

Queda firme en el fallo, que existen determinadas circunstancias que permiten que el Estado deje de lado estos derechos de los ciudadanos en pos de un bien jurídico mayor (como el bien público). El Tribunal de la Corte Suprema ha expresado: *"sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos: 306:1892; 316:703, entre otros)."* En este último justificativo que mencionó el Tribunal, se determinan con claridad las "justas causas" bajo las cuales el Estado podría vulnerar la privacidad de los ciudadanos.

En el precedente de Fallos: 318: 1894 , en el voto de los jueces Fayt, Petracchi y Boggiano, se afirmó que para restringir válidamente la inviolabilidad de la correspondencia, se requiere: a) que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto; d) que dicho medio no sea más extenso que lo indispensable para el aludido logro.

La sentencia de la Corte Suprema de la Nación en el fallo analizado, ha confirmado la declaración de inconstitucionalidad de la Ley 25.873 y su decreto reglamentario 1563/04, que ya se había declarado en las instancias precedentes. En argumento final, la Corte ha dicho que *"es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales."*

Empresas, organizaciones y dependencia tecnológica.

El avance de la tecnología ha brindado a las empresas herramientas y recursos nuevos para poder llevar a cabo varias de las funcionas clásicas de sus negocios.

En este contexto, muchos empleados utilizan los recursos que les brinda la empresa para realizar actividades privadas o personales. Es así que ha surgido la necesidad en los empleadores de buscar alternativas para mantener bajo control estas situaciones.

Un estudio realizado por la operadora de telecomunicaciones NTL: Telewest, afirma que los empleados pierden dos horas diarias por motivo del mal uso de los recursos informáticos.[2]

Desde el campo de la Seguridad de la Información, se observa en la Argentina una tendencia creciente de estos problemas en las empresas y organizaciones públicas. La empresa Symantec ha realizado una encuesta a empleados que perdieron o abandonaron su empleo durante el 2008. El 59% de los ex-empleados admitieron haber robado información confidencial de la compañía, como las listas de contactos de los clientes.[3]

Según PricewaterhouseCooper[4] se sigue invirtiendo una gran cantidad de recursos tecnológicos como cifrado, backup, sistemas de detección de intrusos, firewall, etc., sin considerar como parte del proceso al personal, la estrategia de políticas y la gestión, siendo estos los principales problemas que se enfrentaron con casos millonarios de fuga de información en empresas del TOP 50 mundiales.

En el ámbito laboral, la Ley 20.744, (LCT) omite disponer cualquier referencia explícita al correo electrónico. Surge allí la importancia del análisis e interpretación de los tribunales. A modo de breve repaso de esta Ley, y en el contexto de analizar la legalidad de los controles efectuados por los empleadores, podemos mencionar, entre otras, la obligación del trabajador como del empleador, de obrar de buena fe (art. 63 LCT), las facultades concedidas al empleador de organización (art. 64), de dirección (art. 65); de modificación de formas y modalidades de trabajo (art. 66); de disciplina (art. 67); y de control (art. 70).

A continuación se expone de manera breve y utilizando como recurso la descripción en etapas de la jurisprudencia argentina, con el objetivo de comprender de una manera más profunda el actual estado del derecho de privacidad en el ámbito laboral, visualizando el aumento de las diligencias exigidas a las empresas.

Primera Etapa: Transgresión a los deberes de la LCT.

En un primer momento, la jurisprudencia interpretaba que la utilización indebida de las casillas de correo electrónico de la empresa para fines particulares ajenos al trabajo, configuraba una falta a los deberes de diligencia y buena fe establecidos en la LCT.

En el año 2003, en el caso "G.D.M. del R. c/ YPF s/despido" la Cámara confirmó una Sentencia de Primera Instancia, que había rechazado el reclamo de un trabajador por indemnización de despido sin causa, ya que la Cámara consideró que existía *"una violación al deber de diligencia y buena fe que generaría pérdida de confianza"* al haber utilizado el correo electrónico de la empresa para fines particulares ajenos al trabajo.

[2]The Register: www.theregister.co.uk/2006/05/22/ntl_telewest_misuse/
[3]Symantec: http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20090226_01
[4]PricewaterhouseCooper:http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/PwCsurvey2008_cio_reprint.pdf

Siguiendo la misma línea, en el año 2003 mencionamos el caso de "V.R.I. c/Vestiditos SA s/despido" del Juzgado Nacional de 1ra. Instancia en lo Laboral, con respecto a la situación de hecho que un empleado enviaba mails con contenido pornográfico desde la casilla corporativa, en cuyo fallo se dijo *"Juzgo como suficientemente acreditado que la reclamante utilizó repetida y constantemente su horario y herramienta de trabajo (sistema de correo electrónico de la accionada) pese a las indicaciones que en contrario le fueran reiteradamente impartidas, para recepcionar y reenviar el tan particular y en diversos aspectos objetable material literario y gráfico..."*

Es un fallo importante debido a que la empresa pudo realizar el despido directo del empleado con justa causa, demostrando las indicaciones impartidas y reiteradas al empleado acerca de las condiciones de utilización de los recursos tecnológicos de la empresa.

Como podemos ver en un principio, la utilización inadecuada de los recursos informáticos se interpretaba de un modo más simple, con una interpretación jurídica de que estas situaciones de hecho estaban contempladas dentro de las transgresiones a los deberes impuestos a los trabajadores en la LCT.

Segunda Etapa: Proporcionalidad.

En este segundo período, se puede observar la ampliación de la protección de la privacidad de los empleados en las esferas de las empresas. Esto trae como consecuencia práctica una serie de requisitos necesarios para considerar como justificado el despido del empleado que había incurrido en la mal utilización de los recursos corporativos.

Contextualizados así, se puede traer a cita fallos como "Uhrin, Jorge A. c. Bayer Argentina S.A." de la CNTrab, del año 2003, donde se sostuvo que *"el tráfico informático de material pornográfico en el horario y lugar de trabajo no constituye una injuria de entidad tal que torne procedente el despido del trabajador implicado, toda vez que, ante la ausencia de sanciones previas, es evidente la falta de proporcionalidad entre la sanción aplicada y la falta cometida, correspondiendo en este supuesto la suspensión del trabajador por causas disciplinarias en virtud de la prohibición expresa de la empresa en cuanto a la conducta asumida por aquél."*

También en "Giménez, Victoria c. Crear Sistemas S. A. y otro" de la CNTrab., del año 2003, se dijo *"Es improcedente el despido dispuesto… pues más allá de no haber sido fehacientemente comprobada la conducta que se imputa, aún de tenerse por cierta, no puede soslayarse que si bien el empleador goza de la facultad de imponer sanciones disciplinarias al trabajador desobediente o incumplidor, dicha potestad no debe ser abusivamente utilizada como alternativa válida del despido, no resultando ajustado a derecho que aplique la medida de mayor gravedad en forma intempestiva y sin recurrir previamente a otros medios que la ley le confiere a tal fin."*

De estos fallos se puede extraer uno de los requisitos actuales para lograr la legitimidad de un control o monitoreo por parte de empleador, como lo es la existencia de una proporcionalidad entre la falta cometida por el empleado y la sanción impuesta por tal motivo.

Se puede ver también que en casos de reiteraciones de estas transgresiones a la normativa interna corporativa, se da la entidad suficiente para el despido con justa causa.

Tercera Etapa: Reglamento Interno.

En esta etapa y siguiendo con la tendencia de la anterior, es que se profundiza aún más las exigencias necesarias para legitimar la situación del monitoreo laboral. La existencia de una política de privacidad clara e informada de manera fehaciente al empleado es ahora condición "sine qua non" para ello.

En el caso "Pereyra, Leandro R. c/ Serv. de Almacén Fiscal s/despido", del año 2003, la Cámara Laboral confirmó una Sentencia de Primera Instancia que había hecho lugar a la demanda de despido promovida por el trabajador y había rechazado los argumentos de la demandada, en cuanto ésta alegaba que se trataba de un despido con justa causa por uso indebido del correo electrónico en el lugar de trabajo. El principal argumento del fallo fue que *"la demandada en ningún momento denuncia con precisión cuál es el procedimiento que debió observar el actor en el cumplimiento de sus funciones específicas ni cuáles eran las normas internas y/o las instrucciones impartidas por la patronal sobre el uso de la red informática y, más concretamente, cuál era el control que había implementado sobre el uso del correo electrónico por parte de sus empleados."*

Es entonces requisito indispensable para las empresas contar con un reglamento interno donde se defina con claridad la correcta utilización de los recursos informáticos, junto al establecimiento de sanciones que sean proporcionales a las faltas en que puede incurrir el dependiente.

A modo de refuerzo jurisprudencial, y sin entrar a brindar más en detalles, en la misma línea que los casos anteriores podemos mencionar el caso "Acosta, N. c/Disco S.A." de la CNTrab. del año 2005, "Romero Walter Daniel c/Comsat Argentina SA s/despido" de la CNTrab. del año 2007, donde aparte de señalarse la desproporcionalidad del despido del empleado y la necesidad de la existencia de una política interna expresa, la Cámara exigió además que ese documento debía ser puesto en conocimiento de manera fehaciente y claro a sus destinatarios.

Como hemos podido ver a través de la estrategia teórica de las etapas, en el transcurso del tiempo, la jurisprudencia ha ido afinando los criterios, estableciendo una serie de requisitos indispensables para poder dar lugar al monitoreo laboral, y cuya evolución constante muestra una tendencia al aumento de la protección del eslabón más débil de la cadena: el trabajador y sus derechos fundamentales.

Políticas de Privacidad: Importancia y Riesgos.

Se debe precisar entonces qué son las políticas de privacidad, buscando un concepto conciliador entre los aspectos informáticos y legales. Se las puede definir entonces como un documento que define los principios, reglas, y prácticas de seguridad que realiza una empresa u organización, tendiente a reglar las funciones, deberes, controles y sanciones de su personal, de conformidad con la legislación vigente, las

necesidades de seguridad informática y las finalidades propias de la dirección empresaria.

A través de las mismas, las empresas ejercen su potestad de dictar sus reglamentos internos, definiendo los comportamientos que serán considerados como prohibidos, junto con el establecimiento de un sistema de imputación de sanciones y/o apercibimientos.

En cuanto al contenido de las mismas, este dependerá concretamente de la organización interna que tenga la empresa u organización. No obstante, se podría esbozar a manera de ejemplo, que una política interna standard se compone por una parte general, donde se detalla cuál es su objeto y finalidad, seguido de un apartado de definiciones de conceptos de relevancia, indispensable para una correcta interpretación, ya que delimita así que quedaría subsumido dentro de ese concepto y que no. En la parte especial se definen los roles y funciones dentro de la empresa, identificando deberes y obligaciones, junto con los procedimientos para ejercer y reclamar los mismos. En esta sección, deben mencionarse cuáles son los recursos (no solo informáticos) de la empresa, y cuál es el uso correcto que debe darse a los mismos.

En el correlato de estos artículos, se definirán cuáles son las facultades de control del empleador sobre los empleados, bajo que circunstancias se procederá a realizarse el monitoreo y en qué condiciones.

Por último se debe contar con un sistema de sanciones proporcionales a las faltas incurridas, que pueden consistir en apercibimientos o notificaciones, donde se imputaran al autor o autores de las transgresiones. Es valioso tener en cuenta que en el caso en que la empresa establezca un sistema de sanciones internos, la legitimidad de la aplicación de estas sanciones deberá ser estudiada a la luz de la normativa de la LCT y los estatutos gremiales de cada rama laboral en particular, según los límites del art. 68 de la LCT.

Políticas de Privacidad: Características.

Con lo desarrollado hasta el momento, podemos repasar algunos de los caracteres esenciales que debe poseer el reglamento interno de cualquier empresa u organización:

1. Redacción.
2. Consentimiento.
3. Proporcionalidad.
4. Documentación.
5. Motivación.

Con respecto a la redacción, se dijo que debe realizarse de una manera clara, sin abusar de la terminología técnica, haciéndolo comprensible aún para aquellos empleados que no disponen de una capacitación específica (tanto en la rama de tecnologías de la información como la legal).

Se deberá tener expresado de una manera precisa cuál es el correcto uso de los recursos de la empresa. Al referirse a los "recursos" no solamente se están considerando los informáticos, sino que puede regularse todo tipo de recursos, como la utilización de vehículos de la empresa, maquinarias, etc.

Siguiendo con las características, es exigencia para poder utilizar válidamente las políticas de privacidad en las empresas u organizaciones, contar con el consentimiento expreso y debidamente informado de las personas a las cuál afecta y sobre las cuáles puede ser aplicable el mismo. Con respecto a este tema, más allá de la documentación que muestra de manera fehaciente la aceptación de cada empleado (y la empresa debe guardar el documento entre sus instrumentos legales), se debe comprobar la comprensión clara de las personas sobre las disposiciones impuestas por la empresa (en la mayoría de los casos, se recurren a cursos de capacitación internos para demostrar el cumplimiento de este aspecto). En este sentido, se aplica las consideraciones del deber de información de la Ley de Defensa del Consumidor.

En la actualidad, empresas que ya cuentan con su normativa interna redactada, suelen utilizar como estrategia la de incluir su articulado y aceptación en el mismo contrato de trabajo. Así, desde el momento que las personas forman parte de la empresa, ya dan por consentido el conocimiento de las mismas.

Al realizar la imputación normativa interna de las transgresiones y sus respectivas sanciones, debe existir una relación de proporcionalidad entre las mismas, para evitar llegar a consecuencias graves por faltas menores.

La empresa debe encontrar una relación coherente entre los hechos que transgreden sus normas internas y las sanciones establecidas para los mismos. La importancia radica en que tal transgresión a las normas internas llegue a alcanzar a criterio del juez el carácter de una injuria lo suficientemente grave como para no seguir la prosecución de la relación laboral (art. 242 de la LCT). En caso de no ser así, será considerado despido injustificado y la empresa deberá indemnizar al empleado según esta segunda situación.

Ya ha sido mencionado el concepto de la documentación como carácter necesario de una buena política de seguridad. Con él se esta haciendo referencia a que todos los hechos o incidentes que sucedan, junto con la disposición de sanciones o apercibimientos, debe ser procedimentalizados y documentados, quedando prueba por escrito y consentida por la persona responsable de lo sucedido.

De esta manera, en caso de un futuro litigio, se podrá probar de manera fehaciente actividades o transgresiones anteriores de ese empleado, junto con sus consecuentes intimaciones o apercibimientos por los mismos, dejando fuera de tu toda duda el conocimiento de que los hechos cometidos estaban prohibidos por el reglamento interno.

El quinto elemento: Motivación.

Para poder expresar con claridad este carácter, es necesario que previamente se tenga en claro que considerado dos clases o niveles de control: monitoreo y acceso.

El monitoreo corresponde a un sistema de control general, de nivel medio, amplio, donde las rutinas de vigilancia son establecidas sin objetivos discriminados, de modo aleatorio e impersonal, buscando de manera automática una serie de variables preconfiguradas para mantener todo el sistema (informático o no) bajo un manto de orden y control.

A modo de ejemplo, se puede mencionar los siguientes sistemas de monitoreo informático:

1. Sitios visitados por los usuarios de la empresa (solo se guarda el sitio)
2. Sitios bloqueados por disponer contenido prohibido.
3. Cantidad de datos enviados y recibidos por horario, con registro de usuario.
4. Cantidad de usuarios concurrentes a un sistema.
5. Cantidad de impresiones realizadas por horario, con registro de usuario.
6. Cantidad de almacenamiento utilizado en el servidor por usuario.
7. Frecuencia de modificación de documentos por usuario.

El segundo nivel de control, es el acceso. Se habla aquí de un nivel alto de ejercicio de la potestad de vigilancia del empleador, donde se podría llegar a acceder en la cuenta corporativa de algún empleado en particular, visualizando el contenido de los mensajes que ha enviado y recibido. Es en este nivel, donde existe el mayor riesgo, ya que en el caso de realizarse de manera abusiva o sin el adecuado consentimiento o información, la empresa podría estar configurando del delito de acceso indebido a una comunicación electrónica ajena.

Dejando por sentado la diferenciación entre los dos niveles de control, es que se pasa a desarrollar este último elemento extra como requisito para una buena política de privacidad.

En las políticas internas, se debe tener en cuenta un principio de motivación entre las situaciones de hecho planteadas y sus consecuencias jurídicas. Difiere del carácter de la proporcionalidad en que aquí ya no se habla de la relación coherente de las sanciones, sino que hablamos de un requisito de razonabilidad al momento de definir y establecer los límites y motivos bajo los cuáles serán llevados a cabo los controles sobre los empleados.

Las pautas de control de acceso que pueda llegar a disponer la empresa, deben ser razonables y armonizadas según cada contexto, estableciendo de manera delimitada en qué casos y de qué manera podrá accederse al contenido de las comunicaciones electrónicas.

Debemos preguntarnos entonces ¿el empleador tendría esta facultad de control de acceso permanente e ilimitado a las correos corporativos de sus empleados? o bien, ¿podría acceder a esas comunicaciones sólo en casos delimitados y de entidad suficiente?

Monitoreo Laboral: Teoría de control amplio.

El correo electrónico otorgado a un trabajador como consecuencia de una relación laboral existente, es asimilable a una herramienta más de trabajo que el empleador provee a su empleado, de manera que cuando el correo electrónico sea provisto por el empleador al trabajador en función de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador, independientemente del nombre y clave de acceso que sean necesarias para su uso.

De allí que no puede olvidarse el derecho de propiedad que tiene el empleador sobre esa herramienta que pone a disposición del empleado, como consecuencia del vínculo que los une. Dicha facultad se vincula con las potestades de organización y dirección de la empresa, y sobre todo, con el ejercicio del derecho de propiedad que tiene el empleador sobre las herramientas de trabajo que proporciona a sus empleados.

A consecuencia de ello, esta primera postura, la cual se define como una teoría de control amplio, interpreta que el empleador en base a los derechos arriba mencionados, se encontraría facultado para ejercer el control de monitoreo y acceso sobre toda la información que circule por dicho correo electrónico laboral, sin distinción de situaciones ni contextos especiales que permitan uno u otro nivel de control. Es decir, su potestad de control se resume en un artículo del tipo: *"La Empresa tiene acceso total a todas la cuentas de correo electrónico de su dominio que se usan en todas las computadoras propias"*.

No obstante, esta teoría de control amplio admite que para que las empresas puedan efectuar este control sobre el envío de correos electrónicos por los empleados sin menoscabar el derecho a la privacidad de los mismos es necesario que se informe que se ejercerá esa facultad, contando con el consentimiento de los trabajadores sobre las políticas adoptadas.

Esta postura tiene fundamento principal el que el empleador tiene a su alcance la facultad de control, contemplada en el artículo 70 de la LCT, *"destinada a la protección de sus bienes, siempre salvarguadando la dignidad del trabajador"*. De aquí nace la diferencia entre las dos posturas, precisamente por la mayor o menor amplitud a la hora de la interpretación de esta facultad de control, salvaguardando la dignidad del trabajador.

Monitoreo Laboral: Teoría de control limitado.

En esta postura, denominada teoría de control limitado, se considera que el empleador, contando con una política de privacidad que reúna los requisitos enunciados, podría disponer a modo amplio del control de monitoreo. Sin embargo, se considera abusivo que se ejerza a modo amplio y sin restricción alguna, el nivel de control alto: el acceso a los contenidos de las cuentas corporativas.

Desde esta teoría, el empleador que quiera realizar y ejecutar su potestad de control de acceso, debe cumplir con aquel quinto elemento característico que se mencionaba, la motivación.

Pensemos en el siguiente caso práctico: Juan, trabaja en una empresa X hace varios años, lo ascendieron y le dieron una oficina privada, con su llave, nuevo escritorio con cajoneras, también con cerradura para que pueda guardar sus pertenencias y tener su lugar de trabajo.

Un día Juan llega a su oficina y se da cuenta que han entrado, le han abierto los cajones cerrados y han sacado y leído todo lo que guardaba dentro. ¿Cuál es la sensación? Supongamos que Juan tenía firmada una política de privacidad con la empresa, donde existía un artículo como el que mencionamos (*"La Empresa tiene acceso total a todas los recursos que son de su propiedad"*). Sin dudas que la oficina, el escritorio y los papeles son propiedad de la empresa, sin embargo, ¿no parece excesivo que sin motivo alguno se haya vulnerado el ámbito mínimo de privacidad del empleado? ¿No quedaría vulnerado ese principio de mínima dignidad que protege la LCT? ¿Sigue existiendo una relación de confianza entre empleado-empleador luego de esas muestras de control?

Desde este punto de vista, el ejercicio de la facultad de control más severa, sin fundamentos, se trata de una actitud abusiva, que vulnera una mínima relación de

confianza con el empleado, y que lesiona hasta el más mínimo sentimiento y expectativa de privacidad.

Ahora, en el mismo ejemplo, agreguemos que Juan se ha ido de vacaciones una semana, y algún compañero de la empresa necesita continuar con algún trabajo que él realizaba. ¿Podría acceder a la oficina de Juan y buscar los papeles? Por supuesto, porque existe una necesidad para hacerlo. Existe un motivo.

En el ejemplo mencionado, como situación análoga a la potestad de control de acceso al contenido en todo momento y lugar, se puede apreciar la irrazonabilidad de los medios utilizados por el principal, en situaciones en las que a simple vista, faltan los motivos que ameriten la entidad suficiente para ejercer el nivel más intrusivo de los controles.

El otorgamiento de una contraseña personal y exclusiva genera en el trabajador una expectativa mínima de privacidad (la misma que se generaría al darle la llave de una oficina privada o cajones con llaves propias).

Existiría sin dudas la facultad de control de acceso permanente, en la cuenta de correo general de la empresa (info@empresa.com, legal@empresa.com, ventas@empresa.com), ya que en estos casos, se evidencia que las cuentas no son exclusivas, sino que son de uso colectivo de la empresa o área referida. En el ejemplo sería la situación de un escritorio sin cajones puesto en una oficina general, junto a otros tantos puestos de trabajo, donde tampoco se generaría esa razonable expectativa de privacidad. Con respecto a este punto, más adelante veremos un interesante aspecto a tener en cuenta referido a los delitos informáticos.

En base a lo dicho, es que se propone afinar aún más el lápiz al momento de definir políticas de privacidad, estableciendo en qué casos y con qué justificativos el empleador podría ejercer el control de acceso, delimitando entonces situaciones donde se considere necesario llegar a ese nivel de control. Con ello, y siguiendo un procedimiento previamente documentado y consentido, se acepta el legítimo ejercicio del empleador al control de contenidos sobre esas comunicaciones.

Logrando precisar en qué casos y motivos se podría acceder al control de acceso del contenido, se estaría dejando fuera de toda duda que para ese caso concreto, el acceso al mismo ha sido debido, evitando de esta manera la tipificación penal. En el primer caso, a la luz de un reglamento que permitiera control total sin distinguir ningún tipo de situación, sería más difusa la consideración de que siempre el acceso ha sido debido.

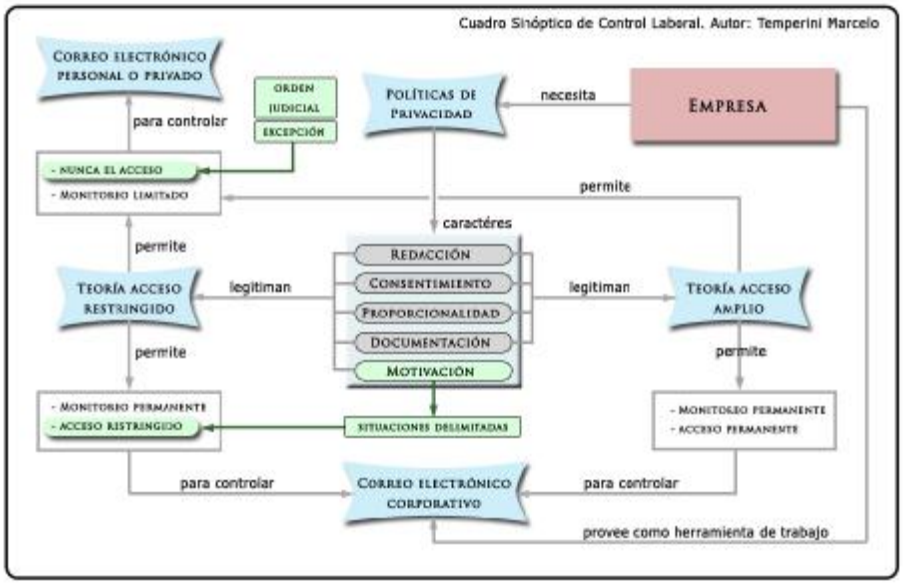
A modo de resumen de fundamentos legales sobre este punto de vista, se toma la mención a los motivos legitimantes para la intervención de la correspondencia, que la Corte Suprema ha sentado precedente en Fallos: 318: 1894, donde se exige que la ley determine con precisión en qué casos y con qué justificativos el Estado podrá realizar la intervención de la información. Razonando esto, se puede inferir que si el Estado, como organismo con el mayor poder en resguardo de los ciudadanos debe respetar las limitaciones de determinar los motivos y situaciones para poder vulnerar la privacidad de los ciudadanos, ¿Por qué el empleador, como sujeto jurídico de menor jerarquía, con menos facultades, podría tener tales atribuciones de injerencia a sus empleados?

La Corte Suprema ha dicho ya que "sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos: 306:1892; 316:703, entre otros).". De manera que se sostiene que

para que exista un control legitimo del empleador en al acceso de manera amplia debe existir una ley que lo permita expresamente. Por el momento, en el tejido normativo argentino, ésta no existe.

Permitir el acceso sin cumplir con los requisitos enunciados, dando lugar a un control total y permanente, vulneraría la prohibición existente en el art. 18 de la Ley 19.728.

Fig. 1.



Correo electrónico Personal y Correo corporativo.

Hasta el momento, todo lo que se dijo acerca de los requisitos necesarios que legitiman el monitoreo del empleador, ha sido con referencia al correo electrónico corporativo, brindado al empleado para realizar sus actividades, y que por lo general (no es condición necesaria), el dominio de la cuenta tendrá el propio nombre de la empresa (por ejemplo marcelo@empresa.com).

En cuentas de correo corporativo, el empleador que cuente con su reglamento interno aceptado y documentado, podría monitorear la actividad de estas cuentas de correo, según las posturas que se desarrollaron.

Ahora, en el caso que el empleado estuviera utilizando una cuenta de correo personal, la situación es diferente. En principio, si en el reglamento interno se expresa que no se podrá utilizar ni revisar cuentas de correo personal utilizando recursos de la empresa, ese empleado estaría cometiendo una de las actividades prohibidas y sería pasible de la sanción prevista.

Se considera que, existiendo una política en donde se exprese que no se puede utilizar cuentas de correo privado desde los recursos de Internet de la empresa, se

podría monitorear la utilización de los recursos por algunos de los métodos vistos, detectando de esa manera si desde algún puesto de trabajo se está violando la normativa. Esto solamente en caso que el empleado, por políticas, haya aceptado y consentido que estaba prohibida la utilización de dichas cuentas. En el caso de no existir el reglamento, sería ilegítimo realizar control de monitoreo.

Bajo ninguna circunstancia, la empresa podría realizar de manera independiente el acceso al contenido de una cuenta de correo personal del empleado.

Aquí puede nuevamente apreciarse la importancia del carácter de la motivación al momento de que la empresa lleve a cabo alguna acción. Es decir, si se sabe que una persona utiliza algo que está prohibido, se debe avisar y sancionar a la persona, pero no acceder y revisar un contenido netamente privado, que conlleva a la empresa a no obtener ninguna utilidad del mismo, además de la comisión de un delito penal.

Pensando en el supuesto de una empresa cuyo empleado está robando información y enviándola a través de su cuenta personal, sería ella una situación de entidad tal, que haga necesario el acceso a esa cuenta de correo privada para comprobar la injuria grave que estaría cometiendo ese empleado.

En estos supuestos, la única alternativa válida para lograrse el acceso, sería previo pedido al juez competente para realizar tal actividad, de manera que solo contando con autorización judicial mediante auto fundado, siguiendo determinados pasos procesales, se podría realizar una pericia de la cuenta de correo privada.

La Privacidad de Empresas y los nuevos Delitos Informáticos.

A partir de la Ley 26.388 se han incorporado y modificado una serie de artículos al Código Penal. Para dejar fuera de dudas qué es lo que se ha buscado proteger, el legislador ha decidido cambiar el título del epígrafe del Capítulo III. Donde decía "Violación de Secretos", podemos ver que ahora dice "Violación de Secretos y de la Privacidad", lo cuál amplía de manera notoria el bien jurídico a proteger.

A través del art. 153 se tipifica y sanciona a aquel que *"abriere o accediere indebidamente a una comunicación electrónica [...] que no le esté dirigido… "*

Sin pretender hacer un análisis exhaustivo desde el punto de vista penal con respecto a este artículo, es de importancia destacar para este trabajo el concepto de realizar una actividad de manera "indebida". El legislador, sólo en este artículo, ha mencionado cuatro veces el mismo concepto normativo, haciendo referencia a la forma o ejercicio antijurídica de la acción.

Se ha dejado a través de este concepto normativo ("indebido"), una puerta abierta para poder incluir allí casos excepcionales, que por las circunstancias concretas, podrían hacer que un tercero acceda debidamente a una comunicación a cuál no le esté dirigida. La pregunta en concreto que debemos hacernos es: ¿Cuándo es indebido el acceso?

A simple vista, podríamos señalar que será indebida la acción, cuando no se tenga derecho para ella. En el caso de las comunicaciones electrónicas, en principio, solo es debido el acceso su destinatario.

Con esta última palabra, planteamos una nueva cuestión. En el caso de un mail corporativo de una determinada persona (por ejemplo marcelo@empresa.com) ¿Se

podría interpretar que más allá del empleado ocasional que trabaja con esa casilla, la empresa es también destinataria de esa comunicación electrónica?

Teniendo en consideración que hemos acordado que el titular de todas las cuentas corporativas, es la empresa u organización, cabría responder de manera positiva, ya que pensando en un sistema organicista de las personas jurídicas, donde las personas son parte de un todo que es la empresa, indirectamente, sería válido decir que la empresa es también destinataria de esa comunicación.

La importancia de tener adoptada esta postura, radica en que si consideramos que la empresa es destinataria (aunque sea indirecta) de esa correspondencia, el acceso a esa comunicación no podría configurar el delito penal tipificado en el 153 (dado que la comunicación también se consideraría dirigida a la empresa, por lo tanto no sería indebido el acceso).

No obstante, más allá de considerar que bajo el velo de esta postura, donde la empresa quedaría fuera del delito penal, seguiría existiendo los límites y consideraciones de respeto hacia el derecho de privacidad del empleado con todas las características que hemos visto.

Derecho Penal en el Derecho Laboral.

Como hemos visto en el desarrollo del trabajo, en el caso de existir una situación de entidad suficiente, sería posible acceder a las comunicaciones de esa persona. Tal circunstancia podría suceder a pedido y con disposición del juez para la interceptación de correspondencia con fines de obtener pruebas para la causa. En ese caso, el acceso sería debido.

En jurisprudencia, es útil recordar el fallo "Grimberg, Alfredo H. s/ sobreseimiento", del la Cámara Nacional en lo Criminal y Correccional de la Capital Federal del año 2003, se decretó la invalidez como prueba de un correo electrónico al que se había accedido ilegalmente. En este caso en particular, se ha desestimado la recepción de un correo electrónico como prueba, dada su ilegitimidad para conseguir el mismo y fue uno de los primeros fallos donde se ha sentado jurisprudencia acerca de los límites existentes para recurrir al ingreso del ámbito privado de una persona, con el fin de poder obtener prueba válida para el pleito.

Es interesante reflexionar en el caso concreto de que una empresa, que sin seguir las diligencias enunciadas en este trabajo, accede indebidamente a las comunicaciones de un empleado. ¿Se configuraría el delito encuadrado el nuevo art. 153? Sabemos que si el Juez laboral, toma conocimiento de estos hechos, tiene la obligación de denunciar el delito. ¿Hasta donde este Juez debe pensar en términos del Derecho Laboral y comenzar a pensar en términos del Derecho Penal? ¿Dónde finaliza el límite para que el juez comprenda de una facultad de control mal realizada, y donde comenzaría el dolo de cometer un delito de acceso indebido a comunicaciones que no le estuvieran dirigidas? De un lado existe el pago una indemnización por daños y perjuicios, del otro, la prisión.

Ahora, si la empresa descubre con ese acceso pruebas de infidelidad laboral reales, aunque ya sabemos que dada su ilegitimidad (caso Grimberg), no podrán ser utilizadas en juicio, ¿Cambiaría en algo la existencia del delito? ¿Podría ser un atenuante del art. 41 inc.?2?

Buscando entre los responsables también hay dudas. Pensemos que sería probable que el administrador de sistemas o de seguridad (por sus conocimientos técnicos), fuera el que en la práctica cometa el delito de acceso o interceptación indebida. ¿Sería autoría simple del administrador de sistemas? Sería razonable pensar que ese empleado actuara bajo directivas o instrucciones de algún superior, ¿Sería ese empleado autor y la empresa un co-autor o instigador? ¿O la empresa sería la única responsable? en ese caso, ¿Podría la empresa ser considerada inimputable según el art. 34 inc. 4 (El que obrare en legítimo ejercicio de un derecho)?

Como vemos, profundizando en estas cuestiones, existen zonas grises donde el Derecho Penal y el Derecho Laboral están demasiado cerca, y en algunos casos llegan a solaparse, dando lugar a diferentes consecuencias jurídicas en base a la aplicación e interpretación de principios y normativas de su propia rama del derecho.

Reflexiones Finales.

Estamos atravesando una nueva etapa, delineada por la proliferante existencia de empresas y organizaciones dependientes de la tecnología, que comienzan a ser concientes de la inseguridad jurídica que las rodea.

Las constantes violaciones a la privacidad de las personas sigue siendo tema de discusión cotidiano, donde este Derecho fundamental toma cada vez más fuerza y nuevas características en su ropaje de constitucional, que junto al principio "in dubio pro operario" sigue siendo el escudo de defensa frente a los embates de control propuestos por las empresas que defienden sus propios intereses.

Donde a falta de regulación específica en la materia, se debe recurrir a la interpretación principios jurídicos básicos, y es el juez quien deberá ponderar en cada caso concreto, cuál es el derecho que debe prevalecer.

Se exige mayor diligencia por parte de las empresas al momento de ejercer sus facultades de control, imponiendo la obligación de delimitar de manera clara y precisa los motivos en las cuales su potestad de control puede avanzar en mayor o menor medida sobre parte de la esfera de privacidad de las personas a su cargo.

Bajo este contexto, sumamos además los interrogantes planteados acerca de la realidad del acercamiento del Derecho Laboral y el Derecho Penal, donde sus límites no son claros, y donde la responsabilidad civil coexiste con la penal en una gran cantidad de situaciones.

Frente a los avances de la tecnología, el derecho debe reaccionar y responder al cambio del estado de cosas que se produce en la sociedad, reflejando esos valores comunes, tal como se expresaba en la teoría clásica de Durkheim.

Es por ello que la intención de este trabajo, es de organizar los hechos que suceden según algunos puntos comunes existentes entre ellos, buscando no sólo comprender la complejidad del problema, sino también abocado a la tarea de proponer y de generar un punto de vista diferente, una alternativa a una realidad que dista de llegar a tener soluciones finales.