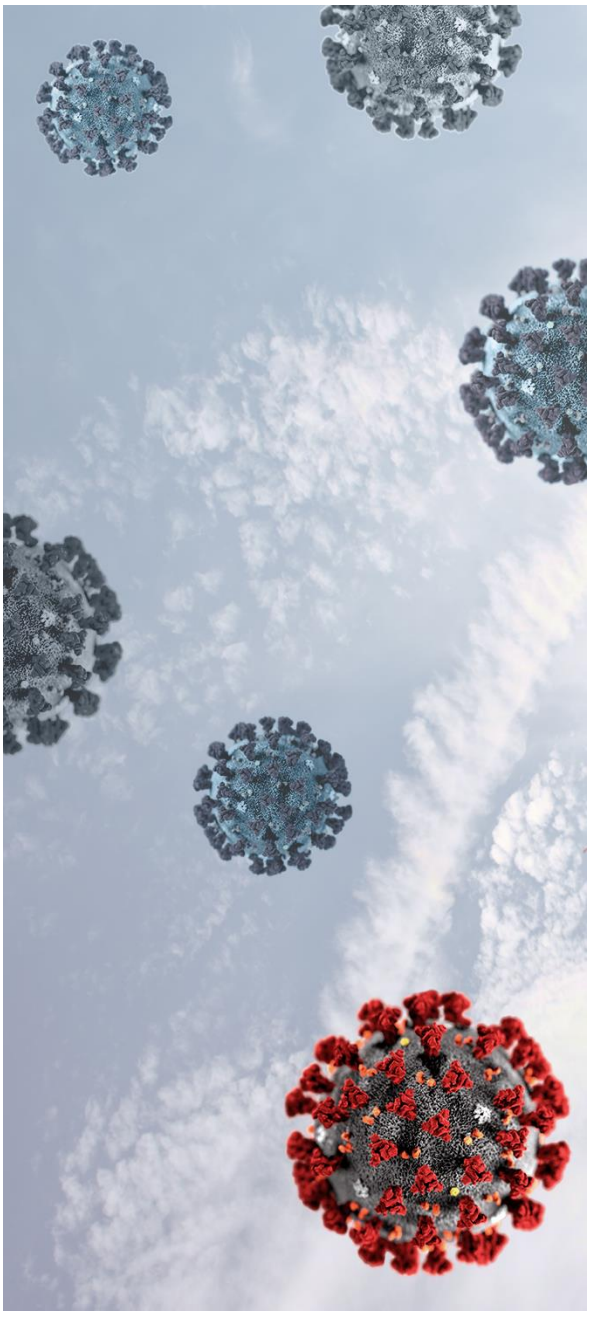
CUATRECASAS

COVID-19: Novedades en materia de protección de datos

Newsletter | Portugal

20 de mayo de 2020



- Orientaciones de la CNPD sobre el control remoto en régimen de trabajo domiciliario
- Orientaciones de la CNPD sobre la divulgación de información relativa a las personas contagiadas por COVID-19
- Orientaciones de la CNPD sobre la recopilación de datos de salud de los trabajadores
- Orientaciones de la CNPD para el uso de tecnologías de apoyo a la enseñanza a distancia
- Orientaciones de la CNPD sobre la recopilación de datos de salud de los alumnos
- Orientaciones de la CEPD sobre el uso de datos de localización y herramientas de rastreo de contactos (*contact tracing*) en el contexto del brote de COVID-19
- Buenas Prácticas de Ciberseguridad en el Trabajo Domiciliario, publicadas por el Centro Nacional de Ciberseguridad de Portugal

I. Orientaciones de la CNPD sobre el control remoto en régimen de trabajo domiciliario

Tras las medidas de confinamiento y distanciamiento social, se ha generalizado el uso del trabajo domiciliario.

En circunstancias normales, las herramientas de trabajo utilizadas por el empleado en régimen de trabajo domiciliario pertenecen al empleador. En este caso, los trabajadores deben cumplir las normas de uso y funcionamiento de los instrumentos de trabajo puestos a su disposición y solo podrán utilizarlos para el desempeño de sus funciones, salvo acuerdo en contrario.

Sin embargo, el carácter excepcional de la situación actual ha hecho imposible que los empleadores pongan recursos tecnológicos a disposición de la mayoría de sus trabajadores. Así pues, los medios utilizados son, a menudo, propiedad de los empleados.

Independientemente de la propiedad de las herramientas de trabajo, en el trabajo domiciliario el empleador sigue manteniendo sus facultades de dirección y control de la ejecución del trabajo. Sin embargo, dado que este régimen no regula el control a distancia, la Comisión Nacional de Protección de Datos (CNPD) señala que "*la regla general que prohíbe el uso de medios de vigilancia a distancia para controlar el desempeño profesional del empleado es plenamente aplicable a la realidad del trabajo domiciliario*". A esta conclusión se llegaría en cualquier caso según la aplicación de los principios de proporcionalidad y minimización de los datos personales.

Así pues, la CNPD subrayó que no se permiten soluciones tecnológicas para el control a distancia del desempeño de los trabajadores, como "*programas informáticos que, además de realizar un seguimiento del tiempo de trabajo y la inactividad, registran las páginas web visitadas, la ubicación del terminal en tiempo real, los usos de los dispositivos periféricos (ratones y teclados), hacen capturas de imágenes del entorno de trabajo, observan y registran cuando se inicia el acceso a una aplicación, controlan el documento en el que se trabaja y registran el tiempo dedicado a cada tarea*".

En opinión de la CNPD, estas herramientas recopilan un exceso de datos personales de los empleados, lo que promueve el control del trabajo en un grado mucho más detallado que el que se lleva a cabo legítimamente en el trabajo presencial en las instalaciones del empleador. En tal medida, la recopilación y el tratamiento de esos datos vulneran el principio de minimización de los datos personales.

No obstante, la CNPD señala que el empleador puede ejercer su facultad para controlar la actividad del empleado de otras maneras; por ejemplo, mediante el establecimiento de objetivos, la creación de obligaciones de presentación de informes con la frecuencia que considere oportuna o la programación de reuniones por teleconferencia, etc.

En cuanto a la necesidad de registrar las horas de trabajo, las soluciones que lo permitan deben limitarse a reproducir el registro realizado cuando el trabajo se realiza en las instalaciones del

empleador (es decir, registrar el comienzo y el final de la actividad laboral y la pausa para la comida). Si no se dispone de tales herramientas, resulta legítimo de forma excepcional que el empleador establezca la obligación de enviar un correo electrónico, SMS o cualquier otro medio que, además de controlar la disponibilidad y las horas de trabajo del empleado, permita al empleador demostrar que no se han superado los horarios máximos de trabajo permitidos por la ley.

II. Orientación de la CNPD sobre la divulgación de información relativa a las personas contagiadas por COVID-19

Presenciamos diariamente la difusión y disponibilidad de información por parte de las autoridades sanitarias sobre los totales nacionales de casos sospechosos, confirmados, recuperados y fallecidos a causa del COVID-19.

Los datos publicados por la Dirección General de Salud ("DGS") son una fuente de información para los municipios, que han publicado información sobre su área territorial con el fin de tranquilizar a sus poblaciones.

En relación con estas publicaciones, la CNPD ha recibido quejas de los ciudadanos, ya que sus datos personales, de identificación y de contacto, incluidos los de menores, se han publicado en las páginas y redes sociales bajo la responsabilidad de las autoridades locales, tras la confirmación del diagnóstico de COVID-19.

En vista de esta situación, la CNPD ha informado de que las autoridades locales no están facultadas a publicar legítimamente datos sanitarios que identifiquen a las personas a las que aluden.

En efecto, *"esta información está sujeta a un régimen jurídico especialmente protegido, dado que corresponde a una categoría de datos personales que puede generar o promover la estigmatización y la discriminación de sus respectivos interesados*". Aunque las autoridades locales alegan la necesidad de conocer y divulgar datos de salud para su misión de garantizar la salud y la protección civil de la población, ese tratamiento de datos depende de una norma legal habilitadora que lo prevea y que proteja específicamente los derechos e intereses de los interesados, y no existe ninguna disposición jurídica de ese tipo.

Otro fundamento de legitimidad en el que podría basarse este tratamiento es el consentimiento de los interesados; que, sin embargo, será difícil de verificar en este contexto. De hecho, en vista de la vulnerabilidad de las personas contagiadas por el virus y su situación de dependencia de la intervención de las autoridades públicas, no se cumplen las condiciones para la emisión de consentimientos libres.

En cualquier caso, la CNPD afirma que *"esa divulgación pública siempre será desproporcionada, por el efecto negativo que tiene en la vida de las personas contagiadas —reiteramos que algunas de ellas son*

menores—, con una restricción excesiva de sus derechos fundamentales, sin que sea posible afirmar que la ventaja directamente derivada de dicha divulgación, en su caso, no se puede conseguir por otros medios menos perjudiciales e intrusivos para la vida privada de las personas".

De igual modo, tampoco podrán publicarse datos sanitarios, incluso sin la identificación de los pacientes, cuando el reducido número de casos en un territorio determinado, en función del tamaño de su población, permita la identificación de las personas contagiadas.

Por consiguiente, las autoridades locales deben abstenerse de adoptar iniciativas que impliquen la recopilación y divulgación de datos personales de sus ciudadanos cuando tales acciones carezcan de fundamento jurídico o no se ciñan a las orientaciones de la autoridad nacional de salud.

III. Orientaciones de la CNPD sobre la recopilación de datos de salud de los trabajadores

Los empleadores han venido adoptando medidas para prevenir el contagio entre sus trabajadores, como la recopilación y el registro de datos sobre la salud y la vida privada de los empleados que puedan apuntar a un contagio por el virus, como la temperatura corporal.

La CNPD recuerda que "*los datos personales relativos a la salud son datos sensibles que revelan aspectos de la vida privada de un trabajador que, en principio, el empleador no tiene por qué conocer, ni debe conocerlos dado que pueden generar o fomentar discriminación*", y que esta categoría de datos está sujeta a un régimen de protección de datos especialmente reforzado, de lo que se desprende que el empleador no conoce, ni puede recopilar o registrar directamente los datos de salud de sus trabajadores.

Pese a que la situación excepcional en la que vivimos ha provocado cambios profundos en el contexto de la prestación del trabajo y la relación empleador-empleado, la necesidad de evitar el contagio por el virus no legitima, sin más, la adopción de cualquier medida por parte del empleador.

En efecto, la prevención del contagio puede justificar la intensificación de las precauciones de higiene, así como la adopción de medidas organizativas relativas a la distribución espacial de los trabajadores o su protección física. Sin embargo, esto "*no justifica la realización de actos que, según la legislación nacional, solo pueden realizar las autoridades sanitarias o el propio empleado, en un proceso de autocontrol*".

Por tanto, la CNPD considera que los empleadores no pueden recopilar y registrar la temperatura corporal de los trabajadores u otra información relativa a su salud o a cualquier comportamiento de riesgo.

No obstante, continúa siendo posible que un profesional de la salud, en el ámbito de la medicina del trabajo, evalúe el estado de salud de los empleados, en particular recopilando, mediante la

cumplimentación de cuestionarios por parte del trabajador, información relativa a su salud o a su vida privada respecto de su salud.

En respuesta a la publicación de estas Orientaciones, la Asamblea de la República dirigió una solicitud parlamentaria de aclaración a la CNPD. En su respuesta, la CNPD reiteró su posición sobre la medición de la temperatura a los trabajadores y enfatizó los siguientes puntos:

- Reafirma que el tratamiento de datos de salud en el contexto de las relaciones laborales, sobre la base del consentimiento del trabajador, es incompatible con el derecho fundamental a la protección de datos y a la intimidad preservados por la Constitución de la República Portuguesa y la Carta de Derechos Fundamentales de la Unión Europea.
- Considera que la disposición contenida en el artículo 13.º-C del Decreto-Ley n.º 10-A/2020, de 13 de marzo, modificado por el Decreto-Ley n.º 20/2020, de 1 de mayo, que prevé la posibilidad de que los empleadores tomen la temperatura corporal a sus trabajadores, no prevé medidas adecuadas para proteger los derechos, libertades y garantías de los interesados que el RGPD impone a los Estados miembros.
- Entiende que el tratamiento de datos de salud sobre la base del interés público según lo recogido en los apartados i) y h) del párrafo n.º 1, artículo 9.º, del Reglamento General de Protección de Datos (adoptado por el Reglamento [UE] 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016) debe ir precedido de una disposición de la legislación nacional o de la legislación comunitaria en la que se definan los supuestos legales para el tratamiento y se determinen las medidas adecuadas para la protección de los derechos y libertades de los interesados.

IV. Orientaciones de la CNPD para el uso de tecnologías de apoyo a la enseñanza a distancia

La CNPD ha publicado orientaciones dirigidas a todos los intervinientes en el tratamiento de datos en el entorno escolar, ya sean profesores, alumnos y padres o tutores, así como aquellos que actúan como responsables o encargados del tratamiento.

La CNPD identifica una amplia gama de datos personales tratados por las tecnologías de apoyo a la enseñanza a distancia: grabación de voz e imagen de todos los intervinientes y terceros, imágenes del interior del hogar, datos insertados en documentos compartidos o en declaraciones verbales realizadas en videollamadas, información en mensajería instantánea y foros.

En lo que respecta a las plataformas de enseñanza, se verifica que se recopilan o pueden recopilarse datos sobre la utilización de las plataformas (metadatos), como el tiempo de permanencia en la plataforma, el número de cursos a los que se asiste, aprobado, etc., y datos personales deducidos de los datos antedichos: capacidades intelectuales, dificultades de aprendizaje, rasgos de la personalidad, datos de salud asociados al intelecto y la concentración.

Según la CNPD, el uso de estas plataformas plantea varios riesgos, a saber:

- Riesgo de uso indebido de los datos recopilados por las plataformas, ya sea por los responsables o los encargados del tratamiento, incluidos los proveedores de servicios de informática en la nube;
- La falta de transparencia en el almacenamiento de datos en el contexto de una posible subcontratación a proveedores de servicios de informática en la nube, lo que da lugar a una pérdida de control por parte de los interesados;
- Tratamiento discriminatorio basado en la definición de perfiles o evaluaciones, en concreto, mediante la toma de decisiones automatizada, basadas en sistemas de análisis del aprendizaje (*learning analytics*), que revisan el rendimiento de los estudiantes;
- El uso de plataformas de comunicación que no garanticen la seguridad de las comunicaciones o cuya configuración incorrecta dé lugar a la divulgación o el acceso no autorizados;
- Riesgo de confidencialidad en el uso compartido de ordenadores;
- Riesgo de que las escuelas y plataformas no rindan cuentas en ausencia de una asignación clara de responsabilidades en el contexto del uso de estas tecnologías;
- Riesgo de vigilancia a distancia con vistas a controlar el desempeño profesional de los profesores (a este respecto, véase el apartado anterior Orientaciones sobre el control remoto en régimen de trabajo domiciliario);
- Riesgo de que los interesados no puedan ejercer sus derechos en las plataformas.

Por consiguiente, a fin de mitigar los riesgos enumerados, la CNPD recomienda la adopción de medidas adecuadas a las tecnologías empleadas, a saber:

- La adopción de cada plataforma de apoyo a la enseñanza a distancia debería ir precedida de una evaluación de los efectos en la protección de datos con vistas a determinar correctamente los riesgos para la privacidad y permitir la adopción de medidas para mitigar esos riesgos. La evaluación puede ser realizada por las entidades que proporcionan y gestionan las plataformas;
- Los profesores deben estar debidamente informados sobre el uso de las plataformas. En particular, deben ser capaces de identificar las configuraciones correctas para garantizar que no haya riesgos para la privacidad de los usuarios, con especial atención a los alumnos;

- Siempre que sea posible, deben elegirse tecnologías que supongan la menor exposición posible del interesado y su entorno familiar (por ejemplo, foros de debate en lugar de videoconferencias);

El uso de cualquier algoritmo de análisis de desempeño (*learning analytics*) debe ser siempre juicioso y realizarse de manera justa y transparente para con los interesados, y exclusivamente si se cumple alguna de las condiciones para la legitimidad de dicho tratamiento.

Es importante destacar en este sentido que ningún centro educativo puede imponer el uso de esta tecnología específica de inteligencia artificial a sus alumnos, y su uso dependerá de una voluntad informada, libre, específica y explícita del alumno o, cuando sea menor, de quien lo represente.

Se proporcionará a los interesados información clara sobre el funcionamiento de los algoritmos de análisis, en particular cuando se trate de decisiones automatizadas. Y debe garantizarse en todo momento el derecho del interesado a obtener intervención humana en ese proceso.

V. Orientaciones de la CNPD sobre la recopilación de datos de salud de los alumnos

La reapertura de los colegios y la reanudación de las clases llevó a varios centros de enseñanza a tomar la temperatura de los alumnos a la entrada a sus instalaciones.

En consonancia con las diversas posiciones públicas ya adoptadas sobre el tratamiento de datos de salud en el marco de la pandemia de COVID-19, la CNPD recuerda que los centros educativos, en su calidad de responsables del tratamiento, deben cumplir los estrictos requisitos para el tratamiento de datos de salud (datos sensibles).

La CNPD también afirma que la reapertura de los colegios, de conformidad con el Decreto-Ley n.º 20-H/2020, de 14 de mayo, no requiere la toma de temperatura, ya que no existe ninguna orientación de la Dirección General de Salud sobre la necesidad y la utilidad de tal acción entre los alumnos.

En consecuencia, la CNPD subraya la necesidad de cumplir los principios generales del tratamiento de datos, a saber, la verificación de una base adecuada para la legitimidad del tratamiento, en los siguientes términos:

- Los centros educativos deben demostrar la existencia de un fundamento legítimo, en virtud de los artículos 5.º y 9.º del RGPD, para el tratamiento de datos sensibles. No bastará con apelar al interés legítimo de terceros, ya que habrá que demostrar que este prevalece sobre los derechos de los interesados, en particular, de menores.

- Por las mismas razones expuestas anteriormente, los centros de enseñanza pública no podrán alegar que el tratamiento es necesario para el ejercicio de funciones de interés público, según lo recogido en el apartado e) del párrafo n.º 1 del artículo 9.º.

- En cuanto a basar el tratamiento de datos en el consentimiento, la CNPD considera que "*toda declaración de voluntad expresada eventualmente por el alumno, o por los padres o tutores, solo es relevante para fundamentar el tratamiento si no existe amenaza o comunicación de que la negativa a someterse al procedimiento de toma de la temperatura corporal conlleva la consecuencia negativa para el alumno de que se le impida el acceso al aula y, por tanto, a las clases necesarias para prepararse de cara a la evaluación*".

- La apelación a la legitimidad del tratamiento no puede basarse en el reglamento escolar, ya que la autonomía de los centros no permite la restricción de derechos, libertades y garantías, en ausencia de acto legal habilitador, concretamente el derecho a la protección de datos personales y la intimidad, preservado por la Constitución de la República Portuguesa y el RGPD.

- Incluso si se demuestra un fundamento legítimo, los responsables del tratamiento deberán atestiguar que este es necesario, en la medida en que sea el medio menos intrusivo para los derechos de los interesados en relación con otras alternativas disponibles.

VI. Orientaciones de la CEPD sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto del brote de COVID-19

En palabras de la Comisaria Europea de Salud, Stella Kyriakides, la lucha contra la pandemia de COVID-19 mediante aplicaciones digitales no prescindirá del "patrón oro mundial" que son la legislación y los valores europeos que protegen los derechos fundamentales, entre los que se encuentran la privacidad y la protección de datos.

En este sentido, el 21 de abril de 2020, el Comité Europeo de Protección de Datos ("CEPD") publicó la Directriz 4/2020 sobre la utilización de datos de localización e instrumentos de rastreo de contactos en el contexto del brote de COVID-19.

Las orientaciones publicadas tienen por objeto aclarar las "*condiciones y principios para el uso proporcionado de los datos de localización y de los instrumentos de localización con dos fines específicos*:

- *apoyar la respuesta a la pandemia mediante la elaboración de modelos de la propagación del virus con vistas a evaluar la eficacia general de las medidas de confinamiento; y*

- *rastrear los contactos y cursar notificación a las personas cercanas a alguien que se haya confirmado como portador del virus, para romper rápidamente las cadenas de contagio*".

El CEPD recuerda que anteriormente había adoptado una postura sobre el tratamiento de los datos de geolocalización, recopilados por un proveedor de servicios de comunicaciones electrónicas, por la que declaraba que estos debían ser anonimizados de antemano.

En cuanto a los datos de localización recogidos directamente de los dispositivos de los usuarios, su tratamiento solo será lícito con el consentimiento previo de los usuarios o cuando el tratamiento sea estrictamente necesario para el servicio de la sociedad de la información solicitado explícitamente por el usuario (por ejemplo, el uso de una aplicación móvil).

El CEPD reflexiona sobre el concepto de anonimización de datos y sus consecuencias jurídicas y técnicas, y llega a la conclusión de que "*existen muchas opciones para la anonimización efectiva, pero siempre con una salvedad. Los datos no pueden ser anonimizados por sí mismos, lo que implica que solo pueden anonimizarse los conjuntos de datos como un todo. En este sentido, cualquier intervención en un patrón de datos único (por medio de la criptografía o cualquier otra transformación matemática) puede, en el mejor de los casos, considerarse una seudonimización*".

En cuanto al rastreo de contactos, el CEDP subraya que el rastreo sistemático y a gran escala de la ubicación y/o los contactos entre personas "*solo puede ser legitimado si hay una adopción voluntaria por parte de los usuarios*". De esta manera, no se contempla como legítima la hipótesis de imponer el uso de esta tecnología a los ciudadanos. El CEDP recuerda la necesidad de que estas aplicaciones se desarrollen en una lógica de privacidad por defecto, respetando los principios de limitación de las finalidades y de minimización de datos.

Los agentes implicados también deben tener en cuenta que puede haber motivos para la legitimidad de un tratamiento de datos que anule el consentimiento, como la búsqueda de un interés público, por parte de las autoridades públicas, según lo establecido en la legislación de la Unión Europea y de los Estados miembros.

Por último, la CEPD subraya que "*los procedimientos y procesos, incluidos los respectivos algoritmos aplicados por las aplicaciones de rastreo de contactos, deberían funcionar bajo la estricta supervisión de personal cualificado a fin de limitar la aparición de falsos positivos y negativos*", y recuerda que el direccionamiento de los posibles infectados "*no debería basarse únicamente en el procesamiento automatizado*".

El CEDP también proporciona un conjunto de recomendaciones y orientaciones, de carácter técnico, sobre el desarrollo de aplicaciones que cumplan el principio de privacidad por defecto.

VII. Buenas Prácticas de Ciberseguridad en el Trabajo Domiciliario, publicadas por el Centro Nacional de Ciberseguridad de Portugal

También informamos que el Centro Nacional de Ciberseguridad de Portugal ha publicado un documento de "Buenas prácticas de ciberseguridad en el trabajo domiciliario" que las organizaciones y empresas cuyos empleados continúan en régimen de trabajo domiciliario han de tener en cuenta.

https://www.cncs.gov.pt/recursos/boas-praticas/

CUATRECASAS

Contactos

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisboa
Praça Marquês de Pombal, 2 (e 1-8º) I 1250-160 Lisboa I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Oporto
Avenida da Boavista, 3265 - 5.1 I 4100-137 Oporto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

Cuatrecasas ha creado el *Task Force Coronavirus*, un equipo multidisciplinar que analiza constantemente la situación actual de crisis surgida a raíz de la pandemia de COVID-19. Para obtener información adicional sobre el contenido de este documento contacte con nuestro *Task Force* a través del correo electrónico TFcoronavirusPT@cuatrecasas.com o con su contacto habitual en Cuatrecasas. Podrá leer nuestras publicaciones o asistir a nuestros seminarios web a través de nuestro *sitio web*.