



¿Qué pasará después del confinamiento? Medidas legales, técnicas y de negocio para la gestión postcrisis

Conclusiones de la videoconferencia organizada por aesYc y
DENAE

- El teletrabajo ha puesto de manifiesto la falta de concienciación en ciberseguridad y los ciberdelincuentes se han aprovechado de ello. A las empresas les ha sorprendido el confinamiento con poca preparación.
- Contra la desinformación en USA no se hace nada y en la UE se legisla con la autoregulación de las plataformas y la formación y cultura de la ciberseguridad y la revolución digital para que la sociedad sepa discernir.
- Hace falta espíritu crítico para atajar la sobrecarga de información y determinar cuál es la información real y veraz y distinguir entre verdad y mentira.
- La tecnología cambiará y humanizará la manera de trabajar, consiguiendo mayor eficiencia, mejorando la conciliación familiar y dejando las oficinas en espacios para acudir a socializar.

Mayo 2020: El teletrabajo ha puesto de manifiesto la falta de concienciación en ciberseguridad y los ciberdelincuentes se han aprovechado de ello, las empresas se han dado cuenta de las ventajas y las oficinas van a empezar a ser un lugar donde se sociabilice y realicen labores que no se puedan hacer en casa por lo que las oficinas tenderán a reducirse y cambiarse.

Estas son algunas de las conclusiones sobre el futuro que nos espera tras el Covid19 escuchadas en la videoconferencia organizada por [Alianza Española de Seguridad y Crisis \(aesYc\)](#) y [DENAE](#), «¿Qué pasará después del confinamiento? Medidas legales, técnicas y de negocio para la correcta gestión postcrisis», moderada por **Norman Heckh**, socio de Ramón y Cajal Abogados y de DENAE, con la intervención de **Borja Moreno**, General Manager de 4iQ, **Vicente Moret**, Letrado de las Cortes Generales, Of Counsel de Andersen Tax & Legal y

Profesor de aesYc y **Mónica Valle**, Periodista especializada en ciberseguridad, fundadora de Bit Life Media y Profesora de aesYc.

Tras superar la pandemia, uno de los mayores retos que tienen las organizaciones es el de entender la nueva situación de los mercados, los cambios legislativos y la manera de tener una reactivación y reinención por medio de la tecnología. Esto solo debería darse siempre bajo una premisa de ciberseguridad y de correcta gestión de riesgos, tanto a nivel operativo, legal y TIC. Así, los intervinientes respondieron a las preguntas ¿Cómo volveremos a la normalidad? ¿Cuáles son los cambios más relevantes a los que nos enfrentaremos? ¿Cuáles serán los nuevos riesgos a los que estaremos expuestos? ¿Cómo va afectar a la operatividad?

La desinformación y cómo regularla

Vicente Moret, habló **sobre la desinformación y los diferentes modelos de respuesta ante el problema**; el de USA que desde el poder público no se hace nada en aras de la libertad de información y la libre expresión sagradas, el de **la UE que si está legislando algo**, al igual que Alemania y Francia por su parte, con una estrategia blanda, que ha comenzado por **la autoregulación de las plataformas, apela a la autoresiliencia de la sociedad y trata de dotar a la población de formación y cultura de la ciberseguridad** y la revolución digital para saber discernir. Desde la UE se pretende Asentar el principio de soberanía digital con la que se protegen los derechos de la persona de manera esencial, y en España, nuestra Constitución ya recoge que la información está amparada siempre que sea veraz, y se apoya en la diligencia del informador siempre que se compruebe que su intención era objetiva.

Para este experto jurista “intentar imponer mediante ley las verdades objetivas es muy complicado porque chocan el derecho a defender la verdad que pueda afectar a personas e instituciones frente a derecho a interpretar opiniones”.

Mónica Valle también habló de la infoxicación y la sobrecarga de información, en realidad de **datos que llegan por todas partes, pero que la información real y veraz es poca y difusa, por lo que no sabemos qué es real o no y no podemos distinguir entre verdad y mentira**. Los usuarios debemos mantener un espíritu crítico y no dejar que nos verifiquen las noticias, sino hacerlo nosotros mismos.

Sobre la privacidad y las apps de geolocalización, no existe ningún dato anonimizado, creo que es prácticamente imposible. A muchos no les importaría facilitar esos datos al Gobierno, al igual que ya se le dan a Google. No podemos olvidarnos de sus seguridad, para evitar la filtración de los datos de los usuarios y más en apps hechas deprisa y corriendo. “estas apps si se implantan con la excusa de del coronavirus no va a haber marcha atrás. Los datos son poder y control y los gobiernos pueden encontrar la manera de que ese control permanezca”.

Digitalización y garantías contra la pandemia

Moret ofreció su visión jurídica sobre la oportunidad de utilizar “herramientas digitales contra la pandemia, pero con garantías”. Para él, en las aprobadas por el Gobierno, una de seguimiento y otra que sí pide datos personales “tenían que haberse implementado garantías excepcionales, mediante una comisión especial que controlar que esas aplicaciones que se van

a desarrollar, porque la UE ha dejado claro que las **garantías de la privacidad** de las personas no desaparecen” con la realidad que estamos viviendo.

Como experto apuntó que la transformación digital sobrevenida por las circunstancias, en el ámbito de las Administraciones Públicas españolas “hay dos velocidades” y puso como ejemplo de una “segunda velocidad” el retraso en este sentido de la Administración de Justicia.

Por su parte, **Mónica Valle**, suscribió que se había producido una **“transformación digital acelerada en todas las empresas que no estaban preparadas**. Solo el 4% en España realizaba teletrabajo; muy por debajo de la media europea” lo que para ella supone un “gran reto sobre todo en materia de ciberseguridad, lo primero a tener en cuenta para evitar riesgos como ciberataques, intrusión en las empresas y robo de datos que están aumentando con esta aceleración. Al estar en casa se relajan los hábitos de seguridad que de por sí no estaban bien implementados en la mayoría de los trabajadores. **El teletrabajo ha puesto de manifiesto esa falta de concienciación y los ciberdelincuentes se han aprovechado de ello.**

Sobre este riesgo **Borja Moreno** explicó que Los cibercriminales desde hace año y medio su negocio superior al del crimen organizado. El ámbito ciber gana al físico. Ahora están en una nueva fase tienen la ventaja de no regirse por la Ley, por lo que con la info que damos en las RRSS y las apps pueden conocer cómo se comporta toda una organización o empresa; para ellos cada vez hay más brechas y les resulta más fácil la suplantación de identidad, de ciudadanos, y de votantes.



Borja Moreno, Norman Heckh, Vicente Moret y Mónica Valle durante la videoconferencia

¿Qué va a pasar tras el Covid?

A la pregunta de ¿qué va a pasar después? Valle insistió en que se deberían cambiar rutinas de empresas y usuarios en cuestiones de seguridad, “porque esto ya lo había previsto Bill Gates, y muchos Hackers previenen de un ciberataque similar al covid-19 pero en nuestra tecnología, no en nuestra salud. Debemos estar preparados para ello”.

Moreno también trató de perfilar un futuro a partir del Covid.19 en cuanto a las nuevas maneras de trabajar. “Algunas medidas seguirán. Habrá que perfilar cuestiones como la seguridad, la privacidad y la relación entre perfiles de trabajo y personales en las redes

sociales, pero **la tecnología cambiará y humanizará la manera de trabajar, consiguiendo mayor eficiencia y mejorando la conciliación familiar**".

Para él, aunque los **medios y herramientas** para teletrabajar llevan mucho tiempo en el mercado, "no se sabían manejar bien; hay falta **de formación** y se ha notado al tener que implantarlo de la noche a la mañana. **Esto afecta a la eficiencia y la eficacia**, que se irán implantando, al igual que un cambio cultural, hacia un mix con más eficiencia entre el teletrabajo y el modelo presencial. Muchas empresas que lo han avanzado dos años. Y algunas administraciones, como la educativa, lo que afecta a la conciliación; se están observando problemas en el ámbito de la seguridad porque los equipos están en manos de niños y toda la familia. La gente no está preparada, no está formada y está trabajando desde casa".

Según Borja Moreno, las empresas se han dado cuenta de las ventajas "y las oficinas van a empezar a ser un lugar donde se sociabilicen empleados, clientes, etc. y más que para trabajar será donde se realicen labores que no se puedan hacer en casa. Las oficinas tienden a reducirse y cambiarse.

En materia de tele educación, **José Javier Martínez**, CISO de la Universidad de Alcalá de Henares y coordinador académico de aesYc, habló de su experiencia con las herramientas continuar con la educación a distancia. Apostó por el video-foro mejor que por webinar para las clases "presenciales" y mostró su preocupación por las cuestiones relativas a la privacidad; "se están utilizando herramientas, por ejemplo de reconocimiento facial, para evaluar a los estudiantes universitarios aunque no son prioritarias para salvar la situación. Por ejemplo, el programa *Proctoring*, es demasiado invasivo, por muy rápido y eficaz que resulte, ya que podría llegar a acumular múltiples demandas" y puso como ejemplo a los alumnos que no tiene cámara y se conectando con su móvil personal para identificarse en un examen) pero, "¿cómo garantizar que estas herramientas dejan de funcionar cuando tú quieres?", cuestionó este experto en protección de datos en el ámbito educativo.

FDO: Marian Álvarez
Comunicación aesYc