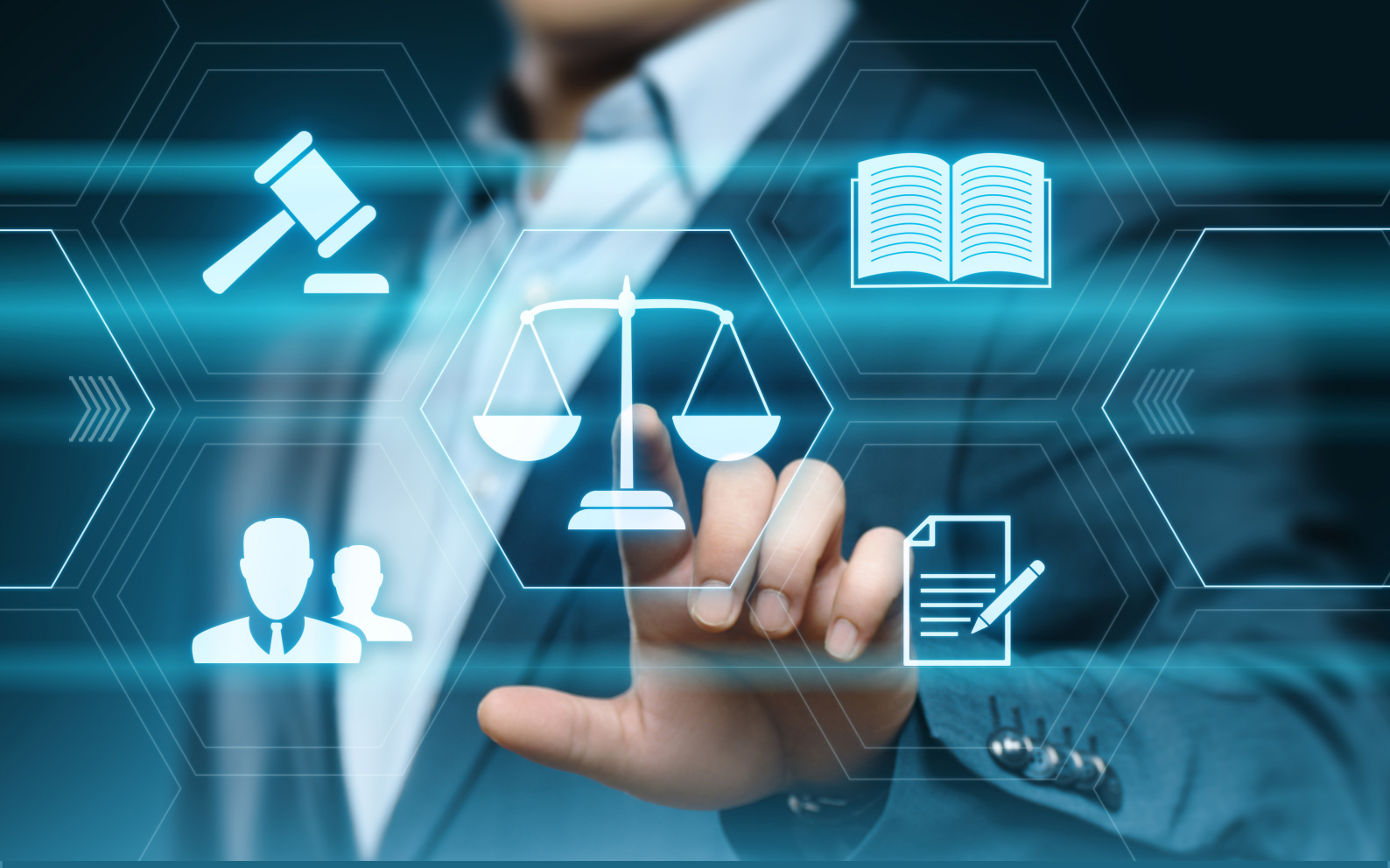


CASOS DE ÉTICA EN EL SECTOR TECNOLÓGICO

"Vale más la buena fama que las muchas riquezas, y más que oro y plata, la buena reputación". (Proverbios 22:1)

Cuando pensamos en tecnología, damos por hecho que las máquinas, los sistemas, no se equivocarán y, en cierta forma, esto es cierto, ya que tanto la parte física (el hardware), como la parte lógica (el software), solo ejecutan las instrucciones que solicitan las personas. Debemos ver la tecnología como una herramienta más, que puede ser usada tanto para el bien como para el mal: a favor o en perjuicio de los demás. Conoceremos desde aparentes decisiones comerciales inofensivas hasta lo más oscuro del sector tecnológico, y las situaciones controversiales que dividen a la opinión pública.

Manipulación de datos: El caso de Volkswagen[1]

En el sector automotriz vimos un caso muy sonado de manipulación de datos por parte de la Volkswagen. La empresa cambió, vía software, los resultados de los controles técnicos de emisiones contaminantes en 11 millones de automóviles con motor diésel, ubicados alrededor del mundo. Estos vehículos emitían hasta 40 veces más contaminantes que los indicados por la normativa. Hasta el momento, la marca alemana va pagando 30,000 millones de dólares debido a sanciones legales y acuerdos realizados. El despres-

Bob, el programador "empresario"[2]

Bob, un empleado norteamericano de perfil bajo, callado, de 40 años, que ganaba cientos de miles de dólares anuales como desarrollador de software, e incluso recibía buenas calificaciones por su excelente desempeño y código limpio. Sin embargo, nadie sabía lo que sucedía detrás de bambalinas. Verizon analizó este caso para la empresa donde trabajaba Bob, y detectó una conexión desde China con las credenciales de Bob. La investigación forense determinó que él subcontrataba a programadores ubicados justamente en China. Según los archivos PDF hallados, Bob invertía la quinta parte de su salario en esta actividad. Finalmente se supo que Bob pasaba todo su tiempo de trabajo consultando sitios de ventas online, almorzando, navegando por redes sociales, viendo videos de mascotas y al terminar su jornada, antes de ir a su casa, informaba sobre los avances realizados.

Creando señuelos online[3]

"Así terminan los que van tras ganancias mal habidas; por estas perderán la vida". (Proverbios 1:19)

En agosto, se conoció el caso de los abogados Paul Hansmeier y John Steele de la firma Prenda, los cuales subían contenido protegidos por copyright a sitios web tipo The Pirate Bay, para luego ir a la cacería de quienes descargaban estos contenidos y conseguir acuerdos judiciales de varios miles de dólares para no exponerlos. The Pirate Bay contribuyó brindando información sobre el modus operandi por medio del cual los abogados llegaron a obtener alrededor de seis millones de dólares en beneficios. En consecuencia, los ahora ex abogados han sido declarados culpables de delitos relacionados con el fraude electrónico y el blanqueo de capitales por los tribunales norteamericanos.

El mundo de los hackers

El hacking, entre los años 1990 y 2000, era cuestión de jóvenes programadores que lo veían todo como un desafío: intrusiones por medio de la ingeniería social como las que realizaba Kevin Mitnick[5] ; ingeniosos gusanos informáticos creados con lenguaje Visual Basic Script, como "I Love You"[6] , que infectaban a todo aquel que abría el archivo adjunto en ese email. Hoy, sabemos que el cibercrimen es más rentable que el narcotráfico. Programadores alrededor del mundo saben que pueden crear malware (software malicioso) y extorsionar tanto a personas naturales como a empresas a fin de que accedan a pagar un rescate por sus archivos cifrados. Justamente, el malware del tipo ransomware es aquel que cifra los archivos de la víctima que, supuestamente, recuperaría lo perdido luego de realizar un pago al hacker por medio de fracciones de Bitcoin. Otro ataque común es el phishing, basado en la ingeniería social, que por medio de emails que pretenden proceder de un familiar, amigo, entidad bancaria, proveedor de servicios u otros, inducen al usuario a ingresar sus datos de acceso a páginas web clonadas de servicios online establecidos legalmente. De esta forma, el usuario envía la información al cibercriminal que desarrolló ese engaño. Los ataques de denegación de servicio (DDoS)[7] también son populares en el ámbito del cibercrímen. Se trata de enviar un inmenso número de solicitudes a un servidor dejándolo sin servicio hasta que cese el ataque. Las empresas que sufren estos ataques se ven obligadas a pagar a los cibercriminales o a contratar servicios de expertos en seguridad informática que mitiguen el ataque y apliquen planes de contingencia. Por otro lado, los dispositivos conectados o Internet of Things (IoT)[8] suponen un reto para la seguridad informática, debido a que para el año 2020 habría unos 50 mil millones de ellos, los cuales no siempre son ideados de forma segura y pueden ser usados como botnets (red de robots informáticos), donde se lleva a cabo ataques DDoS, secuestro de información de wearables (se refiere a la tecnología de uso diario) e incluso el control de dispositivos conectados como automóviles, puertas inteligentes, etcétera. ¿Las empresas asumirán su responsabilidad sobre las brechas de seguridad que se produzcan?

Engañar y manipular la opinión pública

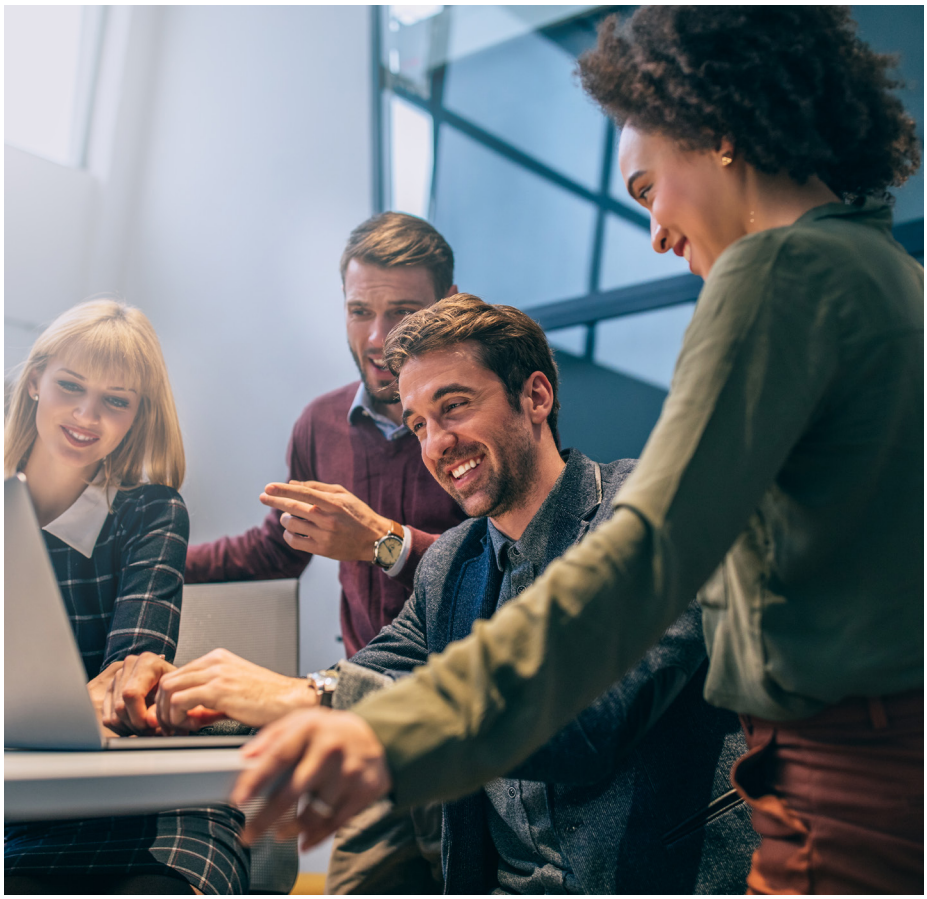
"Dichoso el que halla sabiduría, el que adquiere inteligencia. Porque ella es de más provecho que la plata y rinde más ganancias que el oro". (Proverbios 3:13-14)

La prensa claramente tiene influencia en la población; los usuarios se informan, entretienen y hasta consumen productos o servicios que son publicitados en los espacios respectivos de los medios de información. Sin embargo, hoy es fácil crear una página web y difundir contenidos que no sean reales simulando que lo son. Estas noticias falsas (fake news) no solo crean sorpresa entre los usuarios de redes sociales, también tienen consecuencias graves, como haber ocasionado la muerte de un hombre en Colombia –al que se acusaba de rapto de menores de edad[9]– , que fue atacado a consecuencia de falsas acusaciones a través de la web. En la actualidad, las fake news son consideradas amenazas tan graves como los ciberataques, debido a que arremeten contra la reputación de personas o empresas, produciendo además cuantiosas pérdidas económicas. Este tipo de noticias se generan principalmente en redes sociales. El pensamiento crítico, el cuestionarlo todo, sería de utilidad en estos casos.

Bitcoin, ¿el oro digital?

"El dinero mal habido pronto se acaba; quien ahorra, poco a poco se enriquece". (Proverbios 13:11)

La criptodivisa Bitcoin se hizo famosa el año 2017 debido al crecimiento de su valor, pasando de US$ 1.000 a US$ 20.000 en pocos meses. Su precio actual ha caído hasta los US$ 3.633 . Sus detractores afirman que se usan bitcoins para actividades ilícitas; sin embargo, ¿los dólares americanos, euros u otras divisas están exentos de este uso? Algo que quizá no todos sepan es que Bitcoin sí permite rastrear la ruta del dinero por medio de la tecnología Blockchain; solo debemos consultar por la dirección de la wallet y veremos las fechas, horas, montos y direcciones de otras wallets que fueron parte de esas transacciones. Aprovechándose del poco conocimiento de los usuarios respecto de las criptodivisas, personas inescrupulosas captan a quienes desean invertir, prometiéndoles una alta rentabilidad; sin embargo, los inversionistas no reciben instrucciones de cómo operar en estos mercados, sino son envueltos en estructuras piramidales, y se ven obligados a conseguir cada vez más personas afiliadas. Los métodos de recaudación de fondos colectivos, o crowdfunding[10] , no están libres de personas sin escrúpulos que logran ganarse la confianza de los usuarios para que contribuyan al desarrollo de supuestos productos interesantes e innovadores[11] , que nunca llegan a concretarse: relojes inteligentes, juegos de mesa, un router para navegación anónima, minidrones, entre otros.



Comprando una buena reputación online[12]

"Muchos buscan congraciarse con los poderosos; todos son amigos de quienes reparten regalos". (Proverbios 19: 6)

El eCommerce, concretamente el caso de ventas a través de Amazon, genera grandes beneficios económicos a quienes incursionan en este tipo de negocios. Lo usual es que los emprendedores compren productos de tiendas online de China y las vendan en Amazon, algunos incluso desarrollan innovaciones en los productos base y les ponen su propia marca. Sin embargo, detrás de muchas órdenes de compra y transacciones ocurre algo que pocos imaginan: una falsa buena reputación. La reputación online es muy valiosa y permite generar ventas. Amazon ubica en los primeros lugares de los resultados de búsqueda aquellos productos que tienen varias compras y también reseñas positivas por parte de los compradores. Al existir reseñas negativas, muchos vendedores inician el contacto y ofrecen reembolsos, regalos e incluso dinero a cambio de retirar estas reseñas o cambiarlas por positivas. En otras ocasiones, eran los propios empleados de Amazon quienes eran sobornados para eliminar reseñas negativas a cambio de US$ 300 por cada una.

Popularidad en Google a toda costa

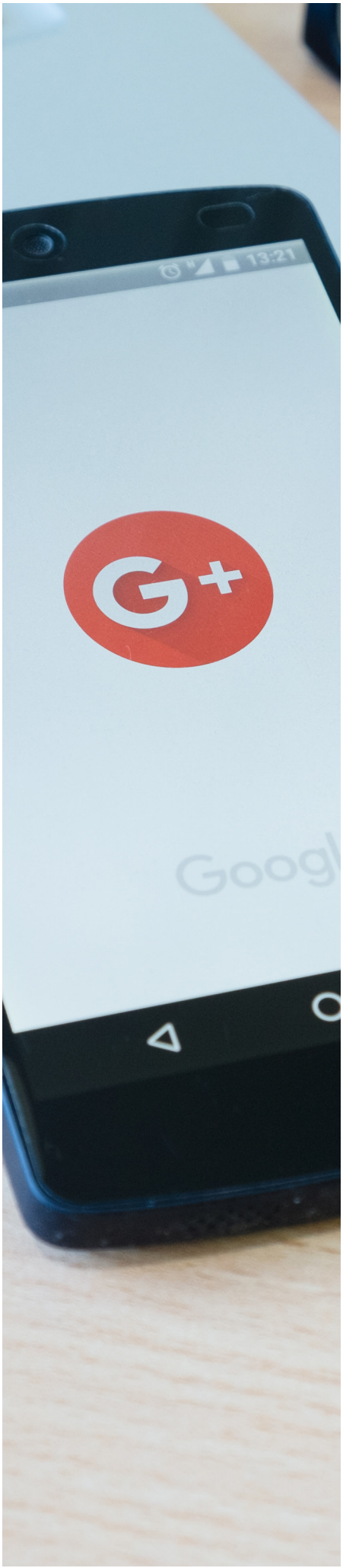
"La tecnología es un siervo útil, pero un amo peligroso". Christian Lous Lange

El Search Engine Optimization (SEO) es el proceso de optimizar contenidos para los motores de búsqueda; es decir, que nuestro sitio web aparezca en los primeros resultados de Google con determinadas palabras clave como las siguientes: viajes, hoteles, comprar smartphones, préstamos personales, etcétera. Si nuestra web aparece entre los primeros resultados obtendremos clics y con ellos potenciales clientes. El Black Hat SEO usa técnicas prohibidas por los motores de búsqueda a fin de evitar que se manipulen los resultados. Para esto se usan textos ocultos, palabras clave repetidas, cloaking (mostrar un contenido a los usuarios, pero otro diferente a los buscadores), comprar enlaces para crecer artificialmente en popularidad. El Black Hat SEO no solo puede ayudar a que una web tome el atajo hacia los primeros resultados de búsqueda, también se usa para hacer SEO negativo hacia los competidores, enlazándolos desde sitios web para adultos, por ejemplo, en donde sufrirían una penalización por parte de Google. Si se combina con fake news, se logra que estas noticias falsas estén en los primeros resultados de ciertas búsquedas. Los cibercriminales usan el Black Hat SEO para engañar a los usuarios de Google, de manera que descarguen archivos infectados creyendo que son archivos legítimos.

¿Sueñan los androides con ovejas eléctricas?

"El espíritu humano debe prevalecer sobre la tecnología". Albert Einstein

Estamos en un momento en el que existe tanto expectativas como incertidumbre respecto al desarrollo de la inteligencia artificial. Watson de IBM colaboró en casos de detección de cáncer de forma exitosa. AlphaGo de Google logró vencer al campeón mundial de Go, entre otros casos. ¿Llegará un momento en que estos sistemas deban tomar decisiones éticas? Ante un inminente atropello, ¿decidirá la inteligencia artifi-



cial atropellar a un anciano o a un niño?[13] , ¿a un hombre indigente o a una mujer ejecutiva embarazada? Mientras aún no se define del todo este escenario, hay esfuerzos como el de la web Moral Machine del MIT[14] , que busca entender las decisiones que tomaríamos los humanos, donde vemos que existen marcadas diferencias dependiendo de nuestra propia cultura.

Fuentes de información:

[1]https://www.bbc.com/mundo/noticias/2015/09/150922_volkswagen_escandalo_trampa_perdidas_ac

[2]https://edition.cnn.com/2013/01/17/business/us-outsource-job-china/index.html

[3] https://confilegal.com/20180822-prenda-law-el-caso-de-un-bufete-americano-donde-los-delincuentes-eran-los-abogados/

[4]https://www.elmundo.es/encuentros/invitados/2008/12/3397/

[5]https://www.elmundo.es/navegante/2001/02/06/entrevistas/981454491.html

[6]https://blog.elevenpaths.com/2013/10/dns-poisoning-gracias-los-sistemas-de.html

[7]http://smoothcommerce.tech/50-billion-iot-connected-devices-by-2020-will-change-business-and-life-as-we-know-it/

[8]https://elcomercio.pe/mundo/actualidad/colombia-muere-linchado-hombre-acusado-robar-ninos-bogota-noticia-nndc-571932

[9]https://www.adslzone.net/2014/10/24/los-mayores-timos-del-crowdfunding/

[10]https://www.xataka.com/empresas-y-economia/seis-proyectos-de-crowdfounding-que-consiguieron-financiarse-pero-despues-fracasaron-estrepitosamente

[11]https://www.elconfidencial.com/tecnologia/2018-10-19/sobornos-amazon-regalos-opiniones-reviews-negativas_1631403/

[12]https://www.xatakaciencia.com/psicologia/mejor-atropellar-a-joven-a-anciano-respuesta-cambia-pais

[13]http://moralmachine.mit.edu/hl/es

Antonio Paredes Romero

Gerente general de Tecnología 21

Alumno de la carrera de Administración