

Universidad Nacional de La Plata  
Facultad de Ciencias Económicas  
Maestría en Dirección de Empresas

**TRABAJO DE TESIS**

Protección y privacidad de la información. Análisis de riesgo y (des)conocimiento en usuarios de TICs de la ciudad de La Plata.

**AUTOR: MAURICIO FOSTER**

**DIRECTOR DE TESIS: EMILIO ZAIMAN**

**LA PLATA, MAYO DE 2020**

## Resumen

Este trabajo de tesis, realiza un análisis detallado del estado de situación actual en lo que refiere a protección de los datos personales (tanto por parte de los dueños de dichos datos, o mejor dicho de quienes los datos refieren, como de las empresas que los recolectan y manipulan) y a la privacidad de la información personal, o a la expectativa de ella que poseen los usuarios de las tecnologías de información y las comunicaciones (en adelante TICs). En particular, pone énfasis en los usuarios radicados en la ciudad de La Plata, de manera de analizar cómo protegen sus datos personales, cuáles son sus expectativas en cuanto a la privacidad, y qué acción realizan (en caso que fuera alguna) en pos de preservarla.

Factores tales como el surgimiento y explosión de las redes sociales que llevaron a nuevas formas de interacción entre las personas, un marco legal deficiente apalancados por una evolución tecnológica de gran escala, hicieron que algo tan relevante como la privacidad de la información personal, quedara relegada por parte de los usuarios de estas nuevas tecnologías. En la actualidad, resulta complejo diferenciar entre datos privados y datos públicos a la hora de hacer uso de las TICs, y es algo que las empresas de tecnología han sabido aprovechar para crear nuevos modelos de negocio perfeccionados con el tiempo y extremadamente rentables en base a la información recolectada de sus usuarios.

El presente trabajo de investigación, se sumerge en el mundo de la protección y la privacidad de la información de los usuarios de TICs, intentando brindar, mediante un lenguaje coloquial y de fácil comprensión, una visión general de lo que está en discusión.

La información se ha convertido en uno de los activos más preciados a todo nivel. Los países desarrollados entendieron que es mediante la información que se hacen diferencias sustanciales frente a los competidores. Términos tales como “guerra de la información” serán cada vez más escuchados. Y estos países ya se lo hicieron saber a sus agencias de inteligencia para que saquen conclusiones acerca del mundo, sin contemplar la ética. Y es así como las nuevas reglas del mundo de la información funcionan.

En la medida que no existan normativas internacionales fuertes que pongan al usuario por sobre las corporaciones o incluso los gobiernos, el derecho a la privacidad será muy débil. Por suerte el mundo empieza a dar señales de vida en la materia, y empiezan a emerger legislaciones que promulgan el derecho a la privacidad como algo básico.

## Palabras Clave

Privacidad, Protección, Información, Tecnología, Comunicaciones, TICs, Usuario, Negocios, Empresas, Internet, Redes Sociales, Hacker, Facebook, Google, Derecho, Concientización, La Plata.

## Tabla de contenido

Resumen .....	1
Palabras Clave .....	2
Introducción: “No hables con extraños” .....	10
CAPÍTULO I: Marco investigativo .....	13
Justificación .....	13
Planteamiento del tema/problema .....	14
Objetivos de la investigación .....	16
CAPÍTULO II: Inicio del Marco teórico .....	17
La privacidad vs “Todo gratis” .....	17
Si no tienes nada que esconder, ¿no tienes nada que temer? .....	19
Algunas definiciones .....	21
Información .....	21
Privacidad (en internet) .....	21
Seguridad de la información .....	22
Qué proteger y de quién .....	23
Nuestra valiosa información .....	23
Reputación online .....	25
Tracking .....	29
Monitoreo en la vía pública .....	30
Hackers .....	33
Gobierno .....	34
Proveedores de Servicio de Internet (ISPs) .....	35
CAPÍTULO III: El Mundo digital. ....	37
Penetración digital en el mundo .....	37
Penetración digital en Argentina .....	39
Un minuto en internet. ....	41

Redes sociales .....	43
Números en el mundo.....	43
Números en Argentina .....	46
Condiciones de Servicio: El ejemplo Facebook.....	49
Google, el oráculo de internet.....	55
Hechos que vale la pena conocer .....	62
¿Qué puedo hacer para protegerme? .....	72
CAPÍTULO IV: Marco legal .....	74
Europa.....	75
Estados Unidos.....	76
Latinoamérica.....	79
Brasil.....	80
Uruguay.....	81
Chile .....	82
Colombia .....	82
México.....	83
Perú .....	84
Argentina.....	84
Censura digital en el mundo.....	90
CAPÍTULO V: El futuro ya llegó .....	94
Internet de las cosas.....	94
5G.....	104
CAPÍTULO VI: Trabajo de investigación de campo.....	106
La privacidad y los negocios .....	106
Supuestos y resultados esperados .....	114
Metodología de la Investigación .....	115
Características de la investigación.....	115

Recolección de datos.....	116
Resultados de la investigación .....	116
Conclusiones .....	148
ANEXO I – Un mundo cada vez más digital.....	156
La explosión de las Redes sociales.....	159
ANEXO II – Condiciones de servicio de Facebook.....	165
ANEXO III – ¿Qué sabe Google de mí?.....	178
ANEXO IV – Argentina. Proyecto de Ley: Ley de protección de datos personales (2018).....	188
ANEXO V - Cuestionario .....	193
Referencias.....	200

## Tabla de Gráficos

Gráfico 1: Privacidad y Seguridad .....	23
Gráfico 2: Sala de Monitoreo La Plata. ....	31
Gráfico 3: Reconocimiento facial (GCBA) .....	31
Gráfico 4: Qué proteger y de quién. ....	36
Gráfico 5: “Digitalidad” en el mundo. ....	37
Gráfico 6: Crecimiento digital anual. ....	38
Gráfico 7: Tráfico de internet por dispositivo.....	38
Gráfico 8: Penetración de internet por región. ....	39
Gráfico 9: Principales datos sobre móviles, internet y uso de redes sociales en Argentina. ....	39
Gráfico 10: Crecimiento digital anual en Argentina.....	40
Gráfico 11: Tiempo empleado en medios (audio, video, internet en general, redes sociales, streaming) en Argentina.....	40
Gráfico 12: Uso de Internet (en Argentina): Perspectiva del dispositivo.....	40
Gráfico 13: Frecuencia en el uso de Internet en Argentina. ....	41
Gráfico 14: Actividades móviles en Argentina. ....	41
Gráfico 15: ¿Qué pasa durante un minuto en Internet? .....	42
Gráfico 16: Visión general de las redes sociales. ....	43
Gráfico 17: Penetración de las redes sociales por región.....	44
Gráfico 18: Penetración de las redes sociales en 2019.....	44
Gráfico 19: Tiempo por día dedicado a las redes sociales.....	44
Gráfico 20: Usuarios activos en las principales redes sociales.....	45
Gráfico 21: Visión general de las redes sociales en Argentina.....	46
Gráfico 22: Plataformas de redes sociales más activas en Argentina. ....	46
Gráfico 23: Audiencia sobre la cual se podría publicitar en redes sociales en Argentina. ....	47
Gráfico 24: Perfil de la audiencia sobre las cuales se podría publicitar en Argentina.....	47
Gráfico 25: Visión general de la audiencia de Facebook en Argentina. ....	47
Gráfico 26: Visión general de la audiencia de Instagram en Argentina. ....	48
Gráfico 27: Página de condiciones de Servicio de Facebook. ....	50
Gráfico 28: Ocurrencia de palabras en la política de Facebook.....	55
Gráfico 29: Evolución de las ganancias de Google.....	56
Gráfico 30: Distribución de las ganancias de Google.....	57
Gráfico 31: Productos de Google "para todos" .....	58

Gráfico 32: Productos de Google "para Negocios" .....	59
Gráfico 33: Productos de Google "para Desarrolladores" .....	59
Gráfico 34: Market share de sistemas operativos para dispositivos móviles en Argentina. ....	60
Gráfico 35: Market share de sistemas operativos para dispositivos móviles en el mundo. ....	60
Gráfico 36: Market share de navegadores (browsers) en Argentina. ....	61
Gráfico 37: Market share de navegadores (browsers) en el mundo. ....	61
Gráfico 38: Dragonfly Eye (Ojo de libélula) .....	63
Gráfico 39: Escándalo Facebook - Cambridge Analytica .....	72
Gráfico 40: Libertad en internet en el mundo. Mapa. ....	92
Gráfico 41: Libertad en internet en el mundo. ....	92
Gráfico 42: Heladera con WiFi.....	95
Gráfico 43: Lavarropas con WiFi.....	96
Gráfico 44: Google Home .....	97
Gráfico 45: Lamparita con WiFi. ....	98
Gráfico 46: Olla de cocción con WiFi .....	98
Gráfico 47: Portero eléctrico con WiFi .....	99
Gráfico 48: Distribución de Proyectos IoT. ....	100
Gráfico 49: Dispositivos conectados IoT en el mundo.....	101
Gráfico 50: Cobertura de 4G en Argentina. ....	104
Gráfico 51: Velocidad promedio de descarga en Argentina. ....	105
Gráfico 52: Velocidad promedio de subida en Argentina. ....	105
Gráfico 53: Latencia de telefonía móvil en Buenos Aires. ....	105
Gráfico 54: Edad de los encuestados.....	117
Gráfico 55: Género de los encuestados.....	117
Gráfico 56: Último estudio concluido de los encuestados.....	118
Gráfico 57: Redes sociales usadas por los encuestados. ....	119
Gráfico 58: Redes sociales usadas por los encuestados, por edad. ....	120
Gráfico 59: Redes sociales usadas por los encuestados, por edad (2da parte). ....	121
Gráfico 60: Publicación de información sensible (encuesta). ....	122
Gráfico 61: Publicación de información sensible, por edad (encuesta).....	123
Gráfico 62: Información considerada privada (encuesta).....	124
Gráfico 63: Información considerada privada, por nivel de estudios (encuesta). ....	125
Gráfico 64: Arrepentimiento sobre lo publicado (encuesta). ....	126
Gráfico 65: Arrepentimiento sobre lo publicado, por edad (encuesta).....	127



Gráfico 66: Uso de facilidades de geolocalización (encuesta). .....	128
Gráfico 67: Uso de facilidades de geolocalización, por edad (encuesta). .....	129
Gráfico 68: Conocimiento de políticas de privacidad (encuesta). .....	130
Gráfico 69: Personalización de configuración de privacidad (encuesta). .....	131
Gráfico 70: Personalización de configuración de privacidad, por edad (encuesta). .....	131
Gráfico 71: Uso de contraseñas (encuesta). .....	132
Gráfico 72: Uso de contraseñas, por edad (encuesta). .....	133
Gráfico 73: Uso de contraseñas, por género (encuesta). .....	134
Gráfico 74: Uso de contraseñas, por nivel de estudios (encuesta). .....	134
Gráfico 75: Conocimiento de robo de información (encuesta). .....	135
Gráfico 76: Conocimiento de robo de información, por edad (encuesta). .....	135
Gráfico 77: Uso de redes WiFi gratuitas (encuesta). .....	136
Gráfico 78: Uso de redes WiFi gratuitas, por edad (encuesta). .....	137
Gráfico 79: Uso de redes WiFi gratuitas, por nivel de estudios (encuesta). .....	138
Gráfico 80: Conocimiento recolección de datos Google (encuesta). .....	139
Gráfico 81: Conocimiento recolección de datos Google, por edad (encuesta). .....	140
Gráfico 82: Conocimiento recolección de datos Google, por género (encuesta). .....	141
Gráfico 83: Conocimiento recolección de datos Google, por nivel de estudios (encuesta). .....	142
Gráfico 84: Opinión cámaras de seguridad (encuesta). .....	143
Gráfico 85: Análisis de los que “Nunca publican nada” (encuesta). .....	145
Gráfico 86: Penetración de internet en 2019. ....	156
Gráfico 87: Tiempo que cada persona pasa por día usando Internet (vía cualquier dispositivo). .....	156
Gráfico 88: Preocupación sobre el mal uso de los datos personales. ....	157
Gráfico 89: Preocupación sobre la privacidad de los datos. ....	157
Gráfico 90: Preocupación sobre las “fake news” en Internet. ....	158
Gráfico 91: Uso de herramientas para el bloqueo de anuncios. ....	158
Gráfico 92: Uso de redes sociales como origen de noticias. ....	159
Gráfico 93: Conectividad móvil en 2019. ....	159
Gráfico 94: Penetración de las redes sociales de población elegible. ....	159
Gráfico 95: Redes sociales: Ranking de “penetración elegible”. ....	160
Gráfico 96: Promedio de cantidad de cuentas en redes sociales. ....	160
Gráfico 97: Promedio de cantidad de cuentas en redes sociales por persona. ....	161
Gráfico 98: Variación en la cantidad de usuarios activos por plataforma social. ....	161

Gráfico 99: Audiencia sobre la cual se podría publicitar en redes sociales. ....	161
Gráfico 100: Ranking de países con las más grandes audiencias para publicitar a través de Facebook. ....	162
Gráfico 101: Ranking de porcentajes de alcance elegible en Facebook. ....	162
Gráfico 102: Perfil de la audiencia para publicitar a través de Facebook. ....	163
Gráfico 103: Audiencia para publicitar con Facebook. ....	163
Gráfico 104: Media mensual de clics por usuario en anuncios de Facebook. ....	163
Gráfico 105: Ranking de países con las más grandes audiencias para publicitar a través de Instagram. ....	164
Gráfico 106: Ranking de países con las más grandes audiencias para publicitar a través de Twitter. ....	164
Gráfico 107: Guardado de actividad de audio y voz de Google. ....	178
Gráfico 108: Dispositivos de Google, con Fit. ....	179
Gráfico 109: Historial de ubicación. ....	181
Gráfico 110: Historial de ubicación de Google. Información que comparte el dispositivo. ....	181
Gráfico 111: Condiciones de servicio de Google. Acceso al correo electrónico. ....	182
Gráfico 112: Configuración de opciones de Google. ....	183
Gráfico 113: Configuración de opciones de Google sobre actividad en la web. ....	185
Gráfico 114: Configuración de opciones de Google. Mis dispositivos. ....	186
Gráfico 115: Descargar mis datos desde Google. ....	186
Gráfico 116: Opciones para configurar controles de actividad. ....	187
Gráfico 117: Portada del cuestionario. ....	193
Gráfico 118: Agradecimiento al encuestado. ....	194

## Introducción: “No hables con extraños”

Tiempo atrás, bajo el lema “No hables con extraños”, se nos inculcaba de pequeños a no dar información a personas desconocidas. Si bien este concepto se mantiene vigente, los cuidados que hace falta tener en la actualidad han cambiado de manera sustancial. Nuestra información puede ser obtenida de varias maneras, y aunque no nos demos cuenta, es altamente probable que cualquier persona de este planeta tenga acceso a una gran cantidad de información nuestra sin que ni siquiera seamos conscientes de ello. Y todo esto, por el sólo hecho de estar conectados a internet, realizando tareas simples como acceder a una página web, buscar algo a través de nuestro motor de búsqueda de preferencia, contar con una cuenta de correo electrónico gratuita, o un perfil en cualquier red social.

La pregunta que a veces me surge para hacerle a determinadas personas que suelen publicar su vida entera en sus perfiles de redes sociales es: ¿Qué información le daría a una persona desconocida que se encuentra de manera fortuita en la vía pública, y que sin ninguna causa razonable le pregunta?:

- Nombre y apellido completos.
- El nombre y apellido completos de sus familiares cercanos.
- La dirección de su domicilio postal. Incluyendo descripción de la fachada de su casa.
- Fecha de su cumpleaños.
- Su equipo de fútbol preferido.
- El partido político con el que tiene mayor afinidad, o en el cual milita activamente.
- Su situación sentimental.
- Su comida preferida.
- El nombre de sus mejores amigos.
- El nombre de su bar o restaurante preferido.
- Lugar y fecha en el que suele pasar sus vacaciones.
- Actividades que realiza en su tiempo libre (con algún detalle de lugar, día y hora).

Seguramente, y en concordancia con el lema que titula este apartado de “No hablar con extraños”, mostrarían una señal de reticencia para dar respuestas veraces a esas preguntas.

Sin embargo, mucha de esa información es publicada de manera abierta en mayor o menor medida por gran parte de los usuarios de redes sociales, sin mucha preocupación, o mejor dicho con total desconocimiento (dado que la preocupación surge en base al conocimiento previo) por el alcance que pueda llegar a tener la misma, o quién pudiera accederla. Pero ¿deberíamos preocuparnos por la cantidad de información que liberamos a la red? Sin duda la respuesta es

un SI rotundo. No es una frase hecha que “todo lo que publicamos en la red, quedará en la red para siempre” sin excepción. Esto significa que una vez que algún contenido es publicado, por más que luego sea modificado, y/o eliminado, en algún lugar ese contenido original permanecerá. O sea que hay que ser extremadamente cuidadoso con lo que se publica.

Por tal motivo, la línea que separa nuestra información pública, de nuestra información privada, suele ser cada vez más delgada y difusa.

La ausencia en la protección de los datos personales, o las bajas expectativas de privacidad, se ponen de manifiesto en gran medida o bien por la falta de conocimiento de la mayoría de los usuarios acerca del tema, o bien porque no se toma el tema con la seriedad que el mismo merece. Y ese es el enfoque que se quiere dar al presente trabajo de investigación. La intención no es generar paranoia en el lector, sino por el contrario crear conciencia de los riesgos que el uso de la tecnología conlleva. Conocer los riesgos, es la mejor manera de cuidarse.

El trabajo de tesis plasmado en el presente documento tiene como metas:

- Introducir al lector acerca de la relación que existe entre el uso de las tecnologías de la información y las comunicaciones, los conceptos de protección de datos personales y la privacidad de la información;
- Analizar las aristas de esta relación, cómo se afectan mutuamente, y en qué impacta la tecnología en el derecho a la privacidad.

La temática aquí desarrollada, se encuentra en una etapa de plena evolución, y dada la modernidad de los temas abordados, no existe contenido teórico que sirva a modo de referencia bibliográfica para sustentar ciertas afirmaciones. En lugar de ello, muchos de los sustentos empleados como fuente, son notas desarrolladas en portales de actualidad tecnológica, informes periodísticos de diarios online de todo el mundo, portales de legislación de distintos países entre otros, pero todos (o en su inmensa mayoría) son contenidos disponibles en la web. De hecho, dado el dinamismo que contiene la temática, algunos de las realidades abordadas cambiaron durante el tiempo en el que este trabajo evolucionaba, haciendo necesario rever algunos de los contenidos ya evaluados. Estos son hechos que todo usuario debería conocer, al menos para tener las herramientas necesarias para decidir en consecuencia.

Es por ello que varios de los capítulos de este documento, tienen por finalidad introducir al lector de la razón por la cual el derecho a la privacidad amerita la presente investigación, y de cómo se llega a este “hoy” en el que muchos países del mundo empiezan a ponerlo como prioridad en sus agendas.

El presente documento de tesis se encuentra estructurado en seis capítulos. El primero de ellos introduce el marco de la investigación en el cual se dejan plasmados tópicos tales como la fundamentación del problema que se analiza, así como también los objetivos de la investigación en sí misma. Estos tópicos son como los basamentos tenidos en cuenta para el inicio de este trabajo de investigación.

Los capítulos II, III y IV hacen en conjunto, las veces de marco teórico para que lector pueda tener el contexto y entender la relevancia de lo que está siendo analizado. Dado que las temáticas a tratar son varias, el CAPÍTULO II pone énfasis en cuál es la información que debo proteger como usuario, y de quién debo protegerme de manera tal de tomar una primera dimensión de los riesgos. Se introducen algunas definiciones de manera de homologar al lector en términos que serán empleados de manera recurrente a lo largo del documento.

El CAPÍTULO III introduce al lector en el cada vez más amplio mundo digital, y en cómo ha logrado penetrar en el mundo para lograr ser hoy lo que es. Para hacer tangible esa penetración, se presentan gráficos con informes realizados por portales online de renombre, a través de los cuales se pretende dar una visión de la dependencia del mundo con la tecnología. Luego se analiza el mundo de las redes sociales, haciendo foco en las condiciones de servicio de Facebook, y un análisis de Google, para mostrar al lector la cantidad de información que posee de los internautas. Entender qué es lo que buscan estas corporaciones y para qué, es de vital relevancia a la hora de usar las TICs. Por último, se analizan varios casos sucedidos en el mundo relacionados con el uso de la tecnología, que dejan a las claras por qué es necesario poner la privacidad de la información de los usuarios (y más que nada el derecho a tenerla) sobre la mesa, y discutir al respecto.

En el CAPÍTULO IV se investiga sobre la diversidad en materia legal relacionada a la temática en países claves del mundo. Se analizan posiciones contrapuestas para luego ver en detalle qué está cambiando en materia legal en varios países, y cómo todo este contexto impacta en Argentina. Se analiza en detalle cómo se posiciona nuestro país en lo que respecta a leyes para amparar el derecho a la privacidad en internet.

El CAPÍTULO V se detiene en ofrecer una breve reseña de qué avances tecnológicos se avecinan (aunque la realidad es que ya convivimos con ellos), de manera de fortalecer la idea de comenzar a tomar cartas en el asunto en referencia a la protección y la privacidad de la información. Se resalta que este documento lejos de querer generar paranoia en el uso de las TICs, tiene por objetivo dar a conocer cuáles son las reglas de juego, quiénes son los jugadores, y qué rol tenemos nosotros como usuarios en este juego para no llevarnos sorpresas en el futuro (y no decir que no sabíamos lo que sucedía).

Por último, el CAPÍTULO VI contiene la investigación de campo a través de la cual se obtienen una serie de conclusiones respecto al grado de conciencia que los usuarios de TICs de la ciudad de La Plata poseen respecto a la protección de su información, y sus expectativas de privacidad sobre la misma. Se brinda el detalle sobre la elaboración de dicha encuesta, así como también todo el análisis relacionado. Además, se analiza de qué manera la temática abordada impacta sobre los negocios, y cómo estos podrían verse afectados en caso de no reaccionar a tiempo en la toma de medidas necesarias para dar tratamiento a la información manipulada.

## CAPÍTULO I: Marco investigativo

### Justificación

El trabajo tiene varios puntos que lo justifican, y varios aportes que le son atribuibles. Para evaluarlo, se tienen en cuenta algunos criterios preestablecidos (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010):

- a) **Conveniencia:** la investigación pretende crear conciencia sobre los riesgos asociados a la sobreexposición de información, ya sea a través de redes sociales, o por el mero uso de dispositivos tecnológicos o software, los cuales, en muchos casos manipulan información sensible de los usuarios sin que estos sean del todo conscientes de ello. De alguna manera, se intenta hacer un llamado de atención a los usuarios de TICs sobre el riesgo en el uso de las mismas.
- b) **Relevancia social:** Con respecto a los mecanismos de protección de la información, y a cómo la privacidad puede ser vulnerada con el uso de las de las TICs, en general los usuarios de las mismas disponen de poco conocimiento sobre, no sólo los riesgos que ello conlleva, sino además de cuál es esa información que se está manipulando en las redes. Por tal motivo, es intención de la presente investigación, aportar un pequeño grano de arena en pos de la concientización en el uso de dispositivos tecnológicos, para que los usuarios tengan una herramienta que les facilite saber cuán importante son sus datos personales (al menos para las corporaciones del mundo) y con qué finalidad los mismos son recolectados. La investigación se presenta en un lenguaje coloquial, de fácil entendimiento para cualquier persona que no disponga de grandes conocimientos relacionados a la informática y/o a la tecnología en general, lo cual facilitará su difusión.
- c) **Implicaciones prácticas:** Con respecto a las implicancias prácticas, la presente investigación tiene dos metas fundamentales:

- Por un lado, analizar el nivel de conocimiento general que los usuarios de la ciudad de La Plata poseen sobre la información que comparten a través de las TICs, y cómo ello podría atentar de manera directa o indirecta sobre la privacidad de la misma.
- Por otro lado, aportar en la concientización no sólo de dichos usuarios, para que, en caso de seguir eligiendo compartir su información a través de las TICs, lo hagan con conocimiento de cuáles son los potenciales riesgos, sino también del mundo de los negocios, para que cuente con herramientas a la hora de tomar decisiones sobre cómo manipulará la poca o mucha información involucrada en sus transacciones.

Estos dos puntos son los que se pretende abordar como aportes pragmáticos.

- d) **Valor teórico:** La presente investigación pretende brindar un importante aporte desde el punto de vista teórico. La temática tiene muchas aristas que se encuentran en constante evolución en el presente, por el cual todos los temas abordados son de extrema actualidad. A su vez, y en base a los estudios previos realizados, se llega a la conclusión que no se cuenta con investigaciones de características similares al abordado en el presente, por lo cual esta investigación podría ser el puntapié inicial para potenciales expansiones, o bien sobre el mismo tema, o bien sobre otros temas relacionados.

### Planteamiento del tema/problema

La evolución de la tecnología es un hecho que desde hace décadas nadie puede desconocer. Esa evolución plantea nuevos paradigmas en la manera en que las personas interactúan, se comunican, conviven entre sí. Nuevos hábitos de vida, nuevos hábitos de consumo cruzados transversalmente por el uso y la penetración tecnológica. Herramientas como el teléfono celular, la computadora en la vida personal y laboral de gran mayoría de la población, han llevado a nuevas costumbres en nuestro día a día. Un buen y simple ejercicio para que el lector internalice su grado de dependencia con la tecnología, es que se detenga a pensar cuán grande sería el desafío de afrontar un día completo de la vida prescindiendo totalmente de su uso. Principalmente de la tecnología orientada a las comunicaciones (teléfono celular u otro dispositivo móvil, computadora, televisor, radio). Y no refiero a pasar un día en lo alto de una montaña en donde la buena señalización de voz o datos podrían verse afectada. La intención es dimensionar en cuanto nuestra rutina se vería afectada, para poder así tener una idea de cuan dependientes somos de la tecnología. Cuántas de las actividades que llevamos a cabo en el día a día dependen del uso de la tecnología.

Lamentablemente hay consecuencias en este uso por momentos excesivo de la tecnología que nosotros como usuarios de la misma, deberíamos conocer. Este documento es producto de un análisis sobre la exposición de los datos personales de las personas, por el uso de las TICs que es así como se denomina al conjunto de herramientas o recursos relacionados con la transmisión, procesamiento y almacenamiento digitalizado de la información.

La distancia ya no es una barrera comunicacional. La idea de la disponibilidad de la información casi sin límites, la facilidad de acceso y la concepción mental sobre la gratuidad de todo lo que se encuentra en la red, llevan al crecimiento de los usuarios de internet año tras año. Y nunca recibimos una capacitación antes de empezar a usar las TICs. Rara vez recibimos consejos acerca de qué sucede cuando “navego” por internet, dónde se almacenan las imágenes que subo, o quién lee lo que escribo. No nos toman examen para configurar las opciones de privacidad de mi perfil de redes sociales. Conceptos desconocidos hace pocos años atrás, tales como redes sociales, hoy conglomeran miles de millones de usuarios que intercambian todo tipo de contenido, muchos de los cuales lucran por realizar acciones malintencionadas. Otro concepto menospreciado por los usuarios es el nivel de exposición de su información en el mundo de la tecnología.

La información se ha transformado en un activo de vital importancia para el funcionamiento de muchos de esos nuevos modelos de negocio, basados, entre otras formas, en el direccionamiento de mensajes publicitarios casi a la medida de cada persona, confeccionados a partir de la recolección de datos de todo el mundo, de manera indiscriminada. La estrepitosa evolución de la tecnología, dejó en evidencia infinidad de vacíos legales, los cuales fueron aprovechados por las compañías para absorber los datos de los usuarios que estuvieran a su alcance (y esforzarse para alcanzar aquellos que no lo estuvieran).

Las nuevas formas de comunicación a través de las TICs, crearon la necesidad de las personas de pertenecer a las comunidades, relegando (o ignorando) cualquier derecho a preservar la privacidad. Además de ello, crearon infinidad de nuevas amenazas que deberían ser conocidas por aquellas personas que hacen uso de las TICs en el día a día de sus vidas. La penetración tecnológica empieza a trascender estratos etarios y sociales para alcanzar a casi toda la población. La desinformación hace que los usuarios sean presa fácil del robo y mal uso de sus datos personales (sean privados o públicos), en muchos casos, sin que ni siquiera sea considerado como una problemática a ser atendida.

Mediante la aceptación de términos y condiciones abusivos, las redes sociales (sólo para citar un ejemplo) creen que es suficiente para hacer lo que se les ocurra con el contenido que sus usuarios generan. Valiéndose de legislaciones pobres o inexistentes, hasta hace poco tiempo lo



venían logrando, teniendo tanta información de sus usuarios que les permiten un nivel de conocimiento inimaginable.

Obviamente, los negocios no están exentos a los cambios que la tecnología introduce. Las TICs están cambiando la manera en que las empresas interactúan con sus clientes y entre sí. Existe una enormidad de ejemplos de cómo la introducción de la tecnología en el negocio, está transformando las reglas y las fronteras. El comercio electrónico, por ejemplo, se ha convertido en herramienta indispensable para la proyección de cualquier tipo de negocio. La globalización hace que las fronteras sean más difusas, y que los potenciales clientes de un negocio, sean el mundo todo.

Todo lo antes descrito lleva a hacernos algunas preguntas:

- ¿Estamos preparados de manera individual, y como sociedad para afrontar los nuevos paradigmas de privacidad que las TICs introducen?
- La necesidad de pertenecer al mundo digital y ser parte de las sociedades que las redes plantean, ¿es más fuerte que mi derecho a preservar la privacidad de mis datos personales?
- El mundo de los negocios, ¿se plantea la necesidad de contar con herramientas y mecanismo para atacar las nuevas necesidades planteadas por un mercado cada vez más necesitado de privacidad en sus datos personales? ¿Qué sucede con los pequeños negocios?
- ¿A qué se exponen las empresas que no adopten las medidas para proveer de seguridad y privacidad a la información que manipulan?

### Objetivos de la investigación

Los objetivos que persigue la presente investigación, se ven plasmados en los puntos que a continuación se detallan:

1. Analizar los riesgos subyacentes en el uso de las TICs respecto a la privacidad de la información.
2. Analizar cómo se comportan los usuarios de la ciudad de La Plata al usar las TICs, en particular en lo que concierne a la protección de “su” información.
3. Determinar el nivel de conocimiento que tienen o creen tener los usuarios de la ciudad de La Plata sobre los riesgos en el uso de TICs relacionado con la privacidad de la información.

4. Evaluar el nivel de preparación que los usuarios de la ciudad de La Plata poseen para enfrentar la evolución de la tecnología.
5. Realizar un análisis comparativo entre diferentes perfiles de usuarios (nivel educativo, rango etario, género, otros) de manera tal de determinar la existencia o no de diferenciación en el grado de vulnerabilidad y de conocimiento en la materia.
6. Brindar al lector herramientas e información de carácter preventivo para la toma de decisiones al utilizar TICs.
7. Analizar cómo pueden incidir en un negocio las decisiones que se tomen respecto a la manipulación de información, y cuál podría ser el impacto de no adoptar mecanismos para abordar la temática aquí tratada.

## CAPÍTULO II: Inicio del Marco teórico

### La privacidad vs “Todo gratis”

Como usuarios de TICs, somos de alguna manera responsables de la pérdida paulatina de la privacidad de nuestra información. Fuimos partícipes necesarios de que hoy estemos hablando de la falta de la privacidad en el uso de las TICs con una alta cuota de responsabilidad. Desde el inicio de internet, la idea que cualquier cosa que yo usara, debía ser absolutamente GRATIS está instalada en nuestra cabeza. Invito al lector a hacer el ejercicio mental de imaginar cuántas de las actividades que a diario realizan a través de internet (o a través de las TICs) dejarían de realizar, si las mismas tuvieran un costo económico asociado. Es decir, si tuviera que pagar dinero para llevarlas a cabo. Seguramente renunciaría a muchas de las actividades que realiza en el ciber mundo hoy de manera “gratuita”. Actividades tales como:

- Descargar e instalar software free.
- Usar una red social.
- Darle like a un comentario.
- Escuchar un tema musical, o ver un video.

¿Cuántas de estas cosas dejaríamos de hacer si tuviéramos que pagar dinero para ello? Imaginen si para leer el diario online, debiera previamente tener una suscripción paga mensual o diaria (obviamente existen diarios online que mantienen un modelo de negocio basado en la suscripción, o bien sólo permiten acceder a un número acotado de noticias sin cargo). Si, tal y como fue siempre con el diario de papel. Sin embargo, esto es hoy algo totalmente inconcebible

en nuestra cabeza. Imaginemos si para crear una cuenta en cualquier red social, debiéramos previamente hacer un depósito desde nuestra tarjeta de crédito, tal como se hace en cualquier club de barrio para mantener nuestra membresía. Y que para mantener esa cuenta viva en el tiempo, sea necesario estar “al día” con el pago mensual. O si para consultar una enciclopedia online, debiéramos previamente hacer un pago para ello. O si debiéramos pagar para ver los videos que tanto nos gustan a través de YouTube. O si los buscadores como Google, tuvieran una cuota en base a la cantidad de búsquedas realizadas. Ni hablar de tener una cuenta de correo electrónico con una suite de herramientas para almacenar archivos en la nube, trabajar con documentos de oficina, y a su vez de manera colaborativa con mi equipo de trabajo entre tantas otras cosas.

Otra revolución tecnológica que nos ayudó a creer que todo en internet era gratis, y que todo debería estar al alcance de todos sin costo (económico) alguno para todos, fue el surgimiento de los programas de tipo punto a punto (P2P peer to peer), en el que los usuarios compartían contenido (películas, música, fotos, programas o cualquier otro que se le ocurra) con el resto de la red, quienes a su vez podían descargarlos casi sin impedimentos (al menos tecnológicos). Podemos citar como gran pionero a Napster que fue el que dio el puntapié inicial para la debacle de las compañías discográficas, y uno de los que obligó a repensar el modelo de negocio de las mismas. A través de este tipo de productos, las personas compartían las pistas de discos completos y podían descargarlos desde las carpetas compartidas por otros usuarios totalmente sin costo (obviamente requería la instalación de un producto de software para gestionar las descargas y para publicar el contenido a compartir). Lo mismo sucedió con las películas. Y podríamos decir que Napster fue sólo el primero de varios, o al menos de los primeros bien conocidos. Sólo para mencionar algunos: Ares, eMule, BitTorrent, Vuze, uTorrent, Kazaa, Audiogalaxy, Morpheus, eDonkey2000. Lo novedoso de estas tecnologías, la dificultad de controlarlas de manera efectiva, la velocidad de su propagación, y la ausencia de un marco legal que pudiera proteger industrias como las de la música, el cine, causaron pérdidas millonarias en dichos mercados. Sólo en Estados Unidos, la industria musical pasó de facturar 7.500 millones de dólares en 1990 a un máximo de 14.600 millones de dólares en 1999 (un crecimiento de casi el 95%), cayendo a partir de entonces a 8.500 mil millones de dólares en 2008 (42% menos respecto a 1999). La disminución en las ventas totales de música coincidió con un gran aumento en el intercambio de archivos de música digital a través de Internet, comenzando con la introducción de Napster en 1999 (Goel, Miesing, & Chandra, 2010).

Lo mismo sucedió con la industria del software. ¿Cuántos de los lectores han pagado alguna vez por la adquisición de un producto de software para instalar en su dispositivo? La idea que todo

debía ser gratis, ha invadido desde hace mucho tiempo a los consumidores de contenido. La tecnología abrió un gran número de puertas a recursos a primera vista "SIN COSTO". Y esto se convirtió en muchos casos, en el primer dominó que cayó para que muchas de las empresas de tecnología revieran su modelo de negocio a implementar y no morir en el intento.

Hoy la mayoría de las transformaciones del modelo de negocios de las compañías basadas en TICs, las lleva al tradicional modelo de venta de publicidad. Y el afán por hacer más eficiente y explotar al máximo las posibilidades de ventas, sumado a nuestra negación por pagar un peso por consumir productos/servicios desde internet, es lo que termina de lapidar nuestras expectativas de privacidad.

Difícilmente la web hubiese evolucionado a lo que es hoy, si esa estructura de clientes que pagan por un servicio hubiera prosperado. Obviamente que la enorme evolución de internet, y el exponencial crecimiento en la cantidad de usuarios y servicios está totalmente relacionado con la "gratuidad" asociada a su uso. Y es algo a lo que tenemos que agradecer. Si los servicios disponibles en la red hubiesen tenido un costo asociado, seguramente su evolución hubiese sido otra, la cantidad de usuarios en sus comunidades sería otra, la oferta hubiese sido otra, la historia hubiese sido otra. No podemos negar que la evolución del mundo en casi todos los ámbitos (tecnología, medicina, educación, ciencias, entretenimiento, etc, etc, etc) le deben en gran parte a este contexto informacional y de libre acceso al que conocemos como internet. Pero claro, todo esto lleva asociado un costo que es el que se trata en este documento: la privacidad de los datos personales de los usuarios.

### Si no tienes nada que esconder, ¿no tienes nada que temer?

¿Es este argumento válido? ¿Es cierto que si no tenemos nada que ocultar, entonces no hay nada de temer? Sin duda que se trata de una pregunta totalmente subjetiva, pero desde mi punto de vista considero que no es así. Pues desde el vamos, es falso que no tenemos nada que ocultar. Pues todos tenemos algo que ocultar. Situaciones de todos los días tan simples como íntimas. Cantar en el auto a viva voz mientras manejamos hacia la oficina, una conversación subida de tono en el grupo de WhatsApp de amigos cercanos en la cual además, se comparte una imagen con un chiste de tinte político. Una charla con un compañero de trabajo sobre el jefe, o sobre otro compañero, un correo electrónico a los docentes de una cátedra, con los ejercicios resueltos del parcial que se tomará el día de mañana, el archivo en el que almaceno las contraseñas del home banking y de mi correo electrónico, los apodos empleados con mis familiares más cercanos en la intimidad. Sin miedo a equivocarme, el 100% de los lectores

preferirán que tanto los eventos antes listados, como la información mencionada queden en el ámbito privadísimo. Y está bien que así sea, pues se trata de información total y absolutamente privada. Y entre otras tantas cosas, es vital la privacidad de las personas en sus vidas.

Edward Snowden hizo alusión a la frase que titula este párrafo, con una genial analogía (Rusbridger, MacAskill, & Gibson, 2015):

“Argumentar que no te importa el derecho a la privacidad por no tener nada que ocultar no es diferente a decir que no te importa la libertad de expresión por no tener nada que decir.”

(En la sección “Hechos que vale la pena conocer”, bajo el título “Los ciudadanos del mundo bajo vigilancia” del CAPÍTULO III de este documento, se trata de manera más detallada sobre este particular personaje).

De hecho, si somos conscientes que estamos siendo observados, seguramente actuemos diferente. De similar manera como actuamos diferentes cuando sabemos que cualquiera de nuestras actitudes, dichos, o lo que fuera que hagamos podrían estar siendo evaluados por alguien más. Seguramente lo mismo haría una persona privada de la libertad en una celda de vidrio, siendo observado por un grupo de personas que se encuentran evaluando su posible libertad. Sabiendo de antemano que se está realizando una evaluación, las actitudes se verían modificadas. Exactamente lo mismo sucede con nuestra privacidad. Simplemente ocultamos ciertas cosas no porque seamos culpables de algo, sino porque son cosas asociadas a nuestra intimidad, a nuestra vida privada y así deberían permanecer.

Sin la añorada privacidad, estaríamos hablando de algo muy parecido a lo expuesto en la película del año 1998 protagonizada por Jim Carrey, “The Truman Show” (Weir, 1998). Algo que para su época resultaba irrisorio y hasta ridículo. Pero mirándolo el día de hoy no estaría tan seguro de calificarlo de esa manera. El avance y la penetración tecnológica, redujeron en gran manera la privacidad o nuestra expectativa a ella asociada a nuestro día a día. Y tenemos que ser conscientes que eso está sucediendo.

Es hora de romper con la idea que, si uno busca privacidad es porque tiene algo que ocultar. Y si tiene algo que ocultar, seguramente sea porque es una persona peligrosa, o sospechosa, al límite de la criminalidad. En algunas ciudades de China, ya se vive como lo hacían los protagonistas de la película citada en donde cada paso, y cada acción tomada es captada por una cámara de video (ver la sección “Hechos que vale la pena conocer”- “Monitoreo en China” en el CAPÍTULO III de este documento para más detalle).

Tenemos que ser conscientes que la totalidad de nuestra vida online, queda registrada en alguna parte. No sólo eso, sino que además nunca se borra, y probablemente nunca se borrará. ¡¡Se guardará para siempre!! Quizás parezca extraño leerlo, pero así es como funciona. ¿Somos capaces de imaginar dentro de 20 años viendo las fotos, videos, audios o cualquier otro contenido subido a algún repositorio online hoy, ya sea por nosotros mismos o por un allegado cercano, con la posibilidad de que además ese contenido pueda ser visto por otras personas? Es difícil de pensarlo o imaginarlo. Pero seguramente toda esa información seguirá existiendo dentro de 20 años, y quizás lo que hoy me resulta simpático, no me resulte de igual forma en el futuro.

### Algunas definiciones

Para iniciar con el análisis, como primera medida es necesario conocer o estar familiarizado con varios conceptos que se irán repitiendo a lo largo del presente documento. Para empezar, es necesario saber de qué se habla cuando hablamos de información, de su protección, de privacidad de la información, la diferencia con respecto a la seguridad de la misma.

#### **Información**

Según el diccionario de la Real Academia Española (Diccionario de la Real Academia Española - Información):

“5. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.”

Según Wikipedia (Información, 2019):

“La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

... es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno.”

#### **Privacidad (en internet)**

Según el diccionario de la Real Academia Española (Diccionario de la Real Academia Española - Privacidad), se define Privacidad (no necesariamente en Internet) como:

“2. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.”

Según el sitio Argentina Cibersegura (Argentina Ciber Segura - Guía sobre Privacidad):

“La privacidad en Internet podría entenderse como el control que ejerce un usuario sobre su información para limitar la cantidad de personas autorizadas a obtenerla. Esto incluye datos personales, fotografías, archivos, etc.”

De manera similar, en un informe de la Internet Society (Society, 2015) declara:

“Aunque no existe una definición de privacidad universalmente aceptada, en el contexto de Internet en general se conviene que privacidades el derecho de determinar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros.”

Por otro lado, según Wikipedia (Privacidad en Internet, 2019):

“La privacidad en Internet se refiere al control de la información que posee un determinado usuario que se conecta a la red, interactuando con diversos servicios en línea en los que intercambia datos durante la navegación. Implica el derecho o el mandato a la privacidad personal con respecto al almacenamiento, la reutilización, la provisión a terceros y la exhibición de información a través de Internet. La privacidad en Internet es un subconjunto de la privacidad de los datos.”

¿Y cuál es la diferencia con el concepto de Seguridad de la Información? ¿Se tratan de lo mismo? La respuesta es NO. Estamos hablando de dos conceptos totalmente diferentes, pero que en muchas circunstancias se complementan. Vemos a continuación la definición de Seguridad.

### **Seguridad de la información**

Para tener una definición formal del concepto, se toma como referencia la norma ISO 27001, en la cual se expresa la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información.

Según Wikipedia (Seguridad de la Información, 2019):

“La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Para el ser humano como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura e idiosincrasia de la sociedad donde se desenvuelve.”

Para entender mejor la diferencia entre seguridad y privacidad, quizás el Gráfico 1 nos pueda ayudar (Belshaw, 2017). A través del mismo se ilustra con una analogía, que en el caso de una casa, la seguridad estaría dada por las cerraduras que uno coloca en las puertas, mientras que la privacidad por las cortinas de las ventanas.

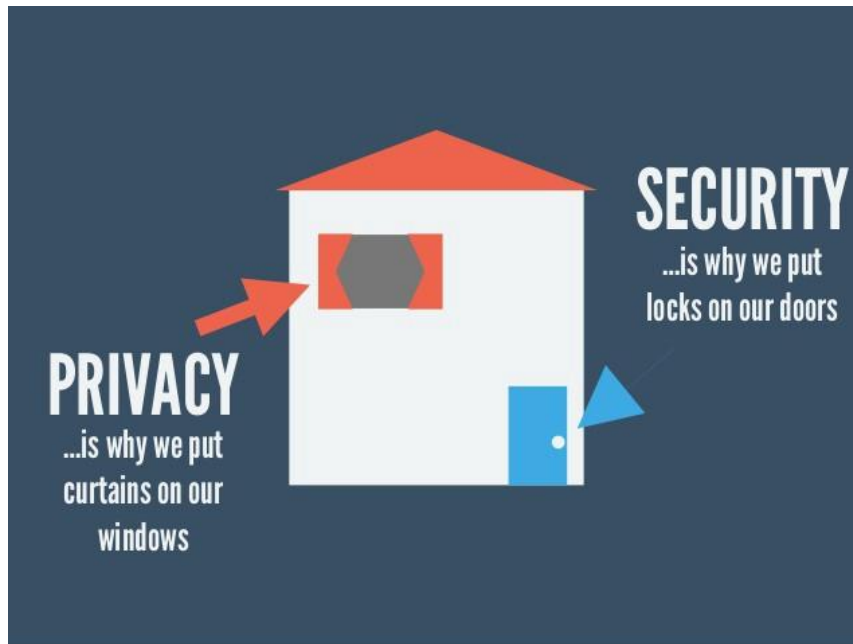


Gráfico 1: Privacidad y Seguridad

### Qué proteger y de quién

A esta altura, el lector debería tener un poco más de claridad acerca de la importancia que posee la privacidad online. Este apartado, introduce otras amenazas que atentan tanto contra la privacidad de la información online de los usuarios de TICs, como amenazas que podrían estar pasando desapercibidas por nosotros, y que, en el mediano o largo plazo, podrían convertirse en un verdadero problema. La intención, es instalar el tema y plantearnos la disyuntiva sobre si lo afrontamos como una problemática, o lo ignoramos como si nada pasara. Pero con conocimiento de que las cosas suceden.

Es algo que tenemos que tener en cuenta todo el tiempo, y no sólo al momento de hacer uso de la tecnología, ya que no sólo es en el ciber mundo, en el cual nuestra privacidad se ve amenazada. Pero hasta aquí, quizás sean cosas sueltas, o tomadas de los pelos. La intención es conocer de manera concreta qué cosas debemos cuidar, qué tipo de información podría ser buscada por un tercero, y quiénes podrían ser esos terceros.

### Nuestra valiosa información



Hasta aquí se trató el tema teórico sobre los riesgos que en el ciber mundo existen. Pero hasta el momento no se hizo mención de qué tipo de información que yo pudiera tener es la que le podría llegar a interesar a un “ciber ladrón”. ¿Cuán relevante es la información que poseo, como para que valga el esfuerzo robármela? Y ante esta pregunta se plantean dos respuestas:

1. No hay esfuerzo, pues les damos toda la información servida en bandeja.
2. Lo suficientemente valiosa como para que las grandes corporaciones como Google y Facebook se estén haciendo millonarias con ella (ver el Gráfico 29 en el que se detalla la evolución de las ganancias de Google, y el Gráfico 30 en donde se informa sobre la distribución de dichas ganancias a modo de ejemplo).

Entonces, cuál es la información que nos podrían sustraer:

- *Contraseñas*: Tenemos montones de ellas. Son la llave para abrir las puertas a nuestra identidad digital: correo electrónico, home banking, redes sociales como para empezar a hablar. Con ellas, cualquiera podría hacerse pasar por nosotros sin mucho esfuerzo y con todo el perjuicio que esto implica.
- *Información financiera*: No caben dudas que este es un platillo que a cualquier ladrón de información le gustaría comer. Si guardamos información del tipo financiera de una manera no segura, esta información podría ser robada por terceros lo cual concluiría en pérdidas económicas como situación extrema. Pero con menor impacto información tal como el detalle de nuestros resúmenes de tarjeta de crédito, el detalle de nuestro recibo de sueldo, las facturas del pago del colegio de los chicos, como tanta otra información de tipo financiera que seguramente elegiríamos mantener en privado y que hablan mucho de nosotros.
- *Información médica*: En nuestro país quizás no sea tan normal contar con registros digitalizados de la historia clínica de una persona. Es algo que se maneja de manera más aislada, o como nicho cada institución médica. Pero supongamos que una persona tuviera un registro médico único. Imaginemos lo grave que sería, y las consecuencias que podría tener para el dueño de esa historia clínica el robo de dicha información, y su posterior divulgación. Nadie estaría feliz con que se dieran a conocer detalles sobre su salud (o ausencia de ella). Sin ir más lejos, si dicha información cayera en manos de su prepaga, o su obra social. Sería la herramienta que les permitiría arancelar la cuota en base a la historia clínica de manera de asegurar rentabilidad con cada persona.
- *Comunicaciones*: En este ítem incluiremos todo tipo de comunicaciones, mensajes de texto, de chat, de mensajería mediante cualquiera de las aplicaciones disponibles para tal fin, intercambio de correos electrónicos, comunicaciones telefónicas, de

videoconferencia, conversaciones personales, etc. Desde siempre, se han buscado mecanismos para buscar la privacidad en las comunicaciones. Hoy día, mecanismos tales como la encriptación de las comunicaciones se han vuelto moneda frecuente, y hasta diría que cualquier comunicación digital que no ofrezca encriptación para proteger su privacidad, casi que debería ser descartada.

- *Metadatos*: Refiere a la información que describe las distintas partes que permiten que uno se mantenga comunicado a través de las TICs. Ejemplo de ello es la información sobre nuestros dispositivos (PC, notebook, teléfono) tal como marca, modelo, características de hardware, de software, capacidad de almacenamiento, etc. Información de la comunicación en sí mismo, ancho de banda, tipo de conexión, etc. Información sobre la red empleada para realizar la conexión, como ser nombre de la red, proveedor, etc. En muchos casos a partir de esta información se puede obtener información adicional, como ser la ubicación desde la cual se realiza la conexión, entre otra.
- *Historial de navegación*: A través del mismo, un sitio puede obtener el comportamiento de los usuarios a la hora de navegar por internet. De dicho comportamiento, podrían inferirse hobbies, gustos, inclinaciones políticas, marcas y comidas preferidas, etc. A partir de esto, se puede crear un perfil del usuario el cual podría ser empleado para orientar la publicidad, o para hacerle llegar contenido con un alto porcentaje de ser acertado para el usuarios destinatario.

### **Reputación online**

En general, todas las personas hacemos un esfuerzo más o menos importante en pos de mantener una reputación cuidada, lo más "limpia" posible. Parte de dicho esfuerzo puede estar centrado en aspectos tales como la vestimenta, la manera de hablar en público, en eventos sociales, los modales, el aseo, la preparación profesional e infinidad de otros aspectos que históricamente repercutieron sobre la reputación de una persona.

Claramente, las vivencias son una parte fundamental de dicha reputación, y a la hora de presentarnos en público, por ejemplo, a la hora de postularnos en un nuevo empleo, seguramente haremos un esfuerzo extra para agradar a la persona que estará frente a nosotros realizando una evaluación de características tales como:

- Nuestra manera de comunicarnos.
- Nuestra pulcritud.
- Nuestra manera de vestir.

- Nuestras posturas o lenguaje gestual.
- Aptitudes para ejercer las tareas correspondientes al empleo.
- Actitudes y/o reacciones frente a diversas situaciones planteadas, que podrían permitirle inferir nuestro comportamiento ante situaciones de crisis.

Y sin duda, la reputación será algo a ser evaluado. Quizás no de manera explícita, pero si de manera implícita todos los reclutadores de recursos humanos para puestos de trabajo, realizan un estudio y análisis minucioso para conocer lo más posible, a los postulantes para cubrir una vacante.

Y créanme que en la actualidad, herramientas para hacer esa evaluación sin siquiera enterarnos, les sobran.

Si el puesto aspirado realmente nos interesa, probablemente hagamos un esfuerzo al momento de ir a la reunión con el reclutador. En cuanto a la vestimenta, en cuanto a la presentación. Ahora, ¿qué sucede con la reputación online? De qué se trata este “nuevo” aspecto al que debemos estar atentos.

Dado que se trata de un concepto subjetivo que no merece una definición formal, se encuentra en Wikipedia, una explicación que encuadra con lo que se desea abordar: “La reputación online es el reflejo del prestigio o estima de una persona o marca en Internet. A diferencia de la marca, que se puede generar a través de medios publicitarios, la reputación no está bajo el control absoluto del sujeto o la organización, sino que la ‘fabrican’ también el resto de personas cuando conversan y aportan sus opiniones. Esto es especialmente importante en Internet, dónde resulta muy fácil y barato verter información y opiniones a través de mecanismos como foros, blogs o redes sociales.” (Reputación Online, 2019)

¿Pero qué cosas podrían afectar mi reputación online? La respuesta a esta pregunta, y teniendo en cuenta que nuestra reputación no sólo estará formada por nuestra actividad, sino que también por la actividad de nuestro entorno o contexto, la realidad termina siendo que casi cualquier actividad en la red podría afectarla.

Un comentario de índole político, o tal vez una broma entre amigos, un comentario desafortunado sobre un compañero de trabajo, o sobre nuestro jefe, o incluso sobre una persona cualquiera. O por qué no la publicación por parte de un amigo, o familiar de una foto tomada en un contexto de confianza como podría ser una reunión familiar, un cumpleaños, un aniversario, una fiesta de fin de año. Además, la misma podría darse a conocer por gran número de canales o medios, por ejemplo, a través de un correo electrónico, en un foro, una red social o incluso una hoja impresa.

Claramente, cada mensaje, cada foto, cada historia, cada conversación, cada posteo está enmarcada en un contexto puntual. El problema empieza cuando los límites entre esos contextos, no sólo dependen de nosotros sino además de todas las personas que lo conforman: nuestros amigos, nuestros familiares, compañeros de trabajo o incluso gente que desconocemos: amigos de nuestros amigos, familiares de nuestros amigos, amigos de nuestros familiares o peor aún, enemigos nuestros o enemigos de nuestros amigos, o enemigos de nuestros familiares. Para ejemplo, tenemos infinidad de casos de fotos subidas por terceros, que hubiésemos querido eliminar. Imagino al lector recordando situaciones en las que se sintió incómodo por una publicación o mensaje electrónico realizado por un tercero.

¿Puede el lector estar completamente seguro que nunca ha publicado o comentado algo sobre una publicación de otra persona de manera inocente, y sin prestar demasiada importancia que pudiera llegar a comprometerlo de alguna manera, ya sea laboral o personalmente? Algo tan simple como una broma quizás un poco subida de tono, o algún comentario político, crítica u observación sobre terceros. O alguna foto personal de vacaciones en la playa con la familia, cena con amigos, reunión de fin de año con compañeros de trabajo, cena de navidad o infinidad de potenciales situaciones que, sin lugar a duda formarían parte de nuestra “intimidad”, de nuestra vida privada, pero que, en las manos incorrectas podrían perjudicar nuestra reputación online. Y la pregunta es, ¿debería preocuparme por ello? Y la respuesta es “Hay que ser precavidos, tomar recaudos”. Y parte de la justificación de dicha respuesta, radica en la infinidad de casos en los que con una simple búsqueda en Google (o cualquier otro motor de búsqueda) de nuestro nombre completo, podríamos llegar a obtener resultados sobre alguno de esos eventos considerados íntimos y personales, que sin duda alguna, elegiríamos que no fueran tenidos en cuenta, ni siquiera visualizados por la persona encargada de realizar la entrevista para ese trabajo nuevo al que nos postulamos, y que tanto nos seduce. Si a eso le sumamos el factor de la baja oferta laboral que se vive hoy día en nuestro país, sepamos que sin dudar, el responsable de recursos humanos, o la persona encargada de realizar la entrevista, “le preguntó a internet sobre nosotros”, para conocer detalles acerca de nuestra reputación online. Y allí, encontrará toda nuestra actividad en redes sociales, nuestros comentarios en foros, en blogs, los comentarios de otras personas sobre nosotros, nuestra actividad profesional, y muchísima otra información de relevancia para cualquier empleador. De hecho, a partir de información publicada en redes tales como LinkedIn, podría conocer de manera aproximada nuestro sueldo actual, variable de gran utilidad a la hora de realizar una propuesta económica. Tenemos la idea que el contenido que subimos a redes como Instagram o Facebook, sólo será de interés para mis amigos y familiares. Que el contenido que subo o genero en redes como LinkedIn, sólo será de

interés y visualizado por aquellas personas que se interesan por nuestra experiencia profesional. Pero lo cierto es que TODA la información está disponible en la red, para que cualquiera la consuma, independientemente de sus intereses.

Sin ir más lejos, y para ilustrar aún más la relevancia que tiene la reputación online, cabe citar un ejemplo bien pragmático. A partir del mes de junio de 2019, y tal como se desprende de artículo periodístico publicado por Clarín (Visa para viajar a Estados Unidos.... en Clarín, 2019), la mayoría de las personas que apliquen a un visado estadounidense tendrán que enviar sus datos de redes sociales junto a sus solicitudes además de proporcionar direcciones de correo electrónico y números de teléfono que hayan utilizado en los últimos cinco años. Este tipo de controles únicamente era exigido a las personas que habían viajado a países y zonas controladas por organizaciones que el país estadounidense tenía catalogadas como "terroristas".

Ahora, con esta información adicional, deberíamos volver a realizar la pregunta que hace algunos párrafos antes se planteó para repensar la respuesta: ¿debería preocuparme por mi reputación online?

Y como para casi todo, existen herramientas en internet que permiten a uno hacer un chequeo sobre el estado de nuestra reputación online, o de una marca (podríamos decir también que nuestro nombre, es la marca que nos identifica personalmente en el mercado profesional). A través de las mismas, se realizan búsquedas de la información disponible sobre la persona, empresa o marca en distintos contextos para concluir cuan positiva o negativa es su reputación online. De requerirlo, se puede contratar además un servicio para mejorar nuestra reputación online. ¿Cómo? A continuación, se cita a modo de ejemplo, el speech empleado por una de las empresas que brinda este tipo de servicios (Gestión de reputación online, 2019):

“Partiendo de la información disponible, tomamos la iniciativa y vamos creando una reputación online positiva mediante el uso de blogs, perfiles profesionales, redes sociales y microblogging: Generamos contenido interesante y se lo hacemos llegar a las personas a las que les interese.... La construcción de una marca tiene unos inmensos costos en publicidad y marketing, y un proceso complejo de creación de campañas publicitarias y de comunicación en medios de todo tipo. En este contexto, Internet y las nuevas plataformas de participación social han dado nuevas y modernas herramientas al internauta para opinar, informar y comunicar”.

En palabras sencillas, lo que realizan es generar contenido positivo sobre nosotros, o sobre nuestra marca. Como el ejemplo antes mencionado hay innumerables sitios web que promocionan servicios de similares características.

Para los lectores cinéfilos, se puede citar un ejemplo de una película de nuestro cine argentino, en la cual se da una situación en la que entra en juego el servicio en pos de mejorar la reputación de una persona. Se trata de la película "Papeles en el viento" (Taratuto, 2015) en la cual, sus protagonistas Fernando (Diego Peretti), Mauricio (Pablo Echarri) y El Ruso (Pablo Rago) pagan a programas de radio influyentes en temas deportivos para que hablen de manera positiva de un mediocre jugador de fútbol en el cual tenían invertida una importante suma de dinero. De esto hablamos cuando hablamos de los servicios para mejorar la reputación.

Respecto a las cosas de las cuales debemos cuidarnos, son muchos los mecanismos en los que nuestra información puede verse comprometida. Muchas de ellas de manera lícita y otras no tanto. Pero casi todos coinciden en su intención de hacerse con nuestra información, en algunos casos sin que siquiera lo percibamos. Vemos a continuación algunos ejemplos de formas en las que nuestra privacidad se ve comprometida. No se trata de una lista exhaustiva, sino sólo de una serie de ejemplos ilustrativos.

### **Tracking**

Cuando hablamos de tracking, nos referiremos al seguimiento que se hace sobre la actividad de las personas cuando hacen uso de internet. Es decir, a la acción de informar a un tercero, sobre aspectos tales como sitios visitados, búsquedas realizadas, tiempo de permanencia en un sitio, imágenes o documentos descargados, características del dispositivo empleado, como marca y modelo del teléfono en caso de hacerlo desde un dispositivo móvil, etc, etc, etc. Toda esta recolección de información es realizada en mayor o menor medida, por la mayoría de los sitios que se encuentran online, y es sin lugar a dudas, una invasión a la privacidad de sus usuarios. Toda esta información recolectada, servirá para entregar a los internautas, entre otras cosas, publicidad con un altísimo nivel de precisión sobre sus intereses. Esto suele lograrse, entre otras cosas, con lo que se denominan cookies, que es una tecnología empleada por casi todos los sitios. Las cookies, son almacenadas por los sitios web en nuestros navegadores y su finalidad es darle al usuario una navegación que se perciba como más "amigable" con el sitio. Por ejemplo, al recordar ciertas preferencias realizadas previamente en el sitio, como ser el lugar desde donde se conecta, el color de fondo de alguna página, la ciudad sobre la que quiere conocer el pronóstico del tiempo (si es que el sitio no lo detecta automáticamente empleando otros métodos). A su vez, los sitios dentro de sus páginas, incluyen código que tienen la función de rastreador y permiten a los sitios recolectar información tal como la que se detallara con anterioridad. Toda la actividad realizada, los comentarios, las búsquedas, los "me gusta" y cualquier otra actividad realizada en línea, será registrada de alguna u otra forma y empleada

para armar un perfil sobre nuestros gustos y brindarnos de esta manera las publicidades que más se ajustan a lo que deseamos.

### **Monitoreo en la vía pública**

Concepto del cual poco se habla, y del que considero hay mucho para decir (o por lo menos para discutir). Con la excusa de mejorar la seguridad, en la mayoría de los Municipios se están instalando cada vez más cámaras de seguridad en la vía pública, las cuales graban de manera constante las 24 horas del día todo el movimiento sobre el que tienen alcance. Lo que se obtiene como resultado, es la vida de gran parte de los ciudadanos almacenada en repositorios sobre los que poco o nada se sabe de la seguridad para que no sea visualizada, o en el peor de los casos robada por terceros malintencionados. Sin ir más lejos, con el foco puesto en la campaña electoral del año 2019, en el sitio web del Municipio de la Plata (Municipio de La Plata - Monitoreo, 2019) uno de los focos está planteado en su centro de monitoreo. A su vez, este Municipio (sólo para citar uno como ejemplo, porque se trata de una política común para todos) anuncia la instalación de 1000 (Diario Ámbito - Centro de Monitoreo La Plata, 2019). En la nota se menciona que:

“El nuevo Centro de Monitoreo contará con un plantel de 170 personas, capaces de visualizar las 320 cámaras instaladas en la ciudad, e incorporará más personal a medida que el Municipio avance con la instalación de más dispositivos, hasta completar el objetivo de 1000 antes del mes de agosto.”

A través del Gráfico 2 puede visualizarse la Sala de monitoreo del Municipio de la ciudad de La Plata (Fuente: Prensa Municipio de La Plata)



Gráfico 2: Sala de Monitoreo La Plata.

Nada se menciona en la nota acerca de las políticas de privacidad, de almacenamiento, de los convenios de confidencialidad (en caso que hubiere) que hacen firmar a los operadores acerca de toda la información a la que tuvieran acceso.

Cabe destacar además, que mediante Ordenanza 11.623 (Concejo Deliberante La Plata, 2017), la Municipalidad de La Plata permite a todas aquellas personas o comerciantes con domicilio en el partido de La Plata, adherirse al programa instalando cámaras de seguridad en sus casas o comercios, y compartir el monitoreo de las mismas con el centro de monitoreo municipal.

A lo antes expresado hay que sumarle lo ya implementado en la Ciudad Autónoma de Buenos Aires, mediante la instalación de por lo menos 300 cámaras de seguridad entre otros lugares, en calles y estaciones de subte con tecnología que permite hacer reconocimiento facial de las personas que son captadas por las mismas. (GCBA - Reconocimiento Facial, 2019)

El Gráfico 3 ilustra cómo sería el sistema de referencia (Fuente: Sabrina Montero y Martín Macagno - GCBA)

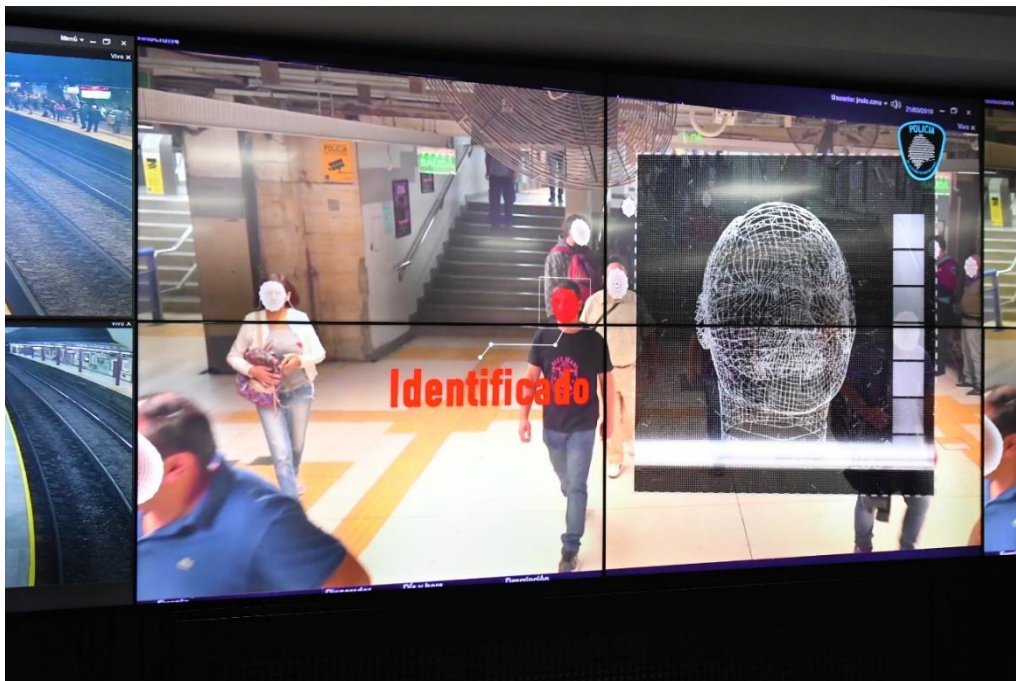


Gráfico 3: Reconocimiento facial (GCBA)

Esta nueva tecnología recientemente implementada ha despertado no pocos rechazos en la sociedad que brega por sus derechos a la privacidad.

Desde la ONG Asociación por los Derechos Civiles (ADC), que según la información provista en su portal (Portal ADC, 2019) “promueve los derechos civiles y sociales en la Argentina y otros



países latinoamericanos”, se ha presentado una solicitud de información pública al GCBA, de detalles sobre la implementación de dicho sistema. Detalles técnicos del sistema, así como aspectos legales sobre los que se sustenta, pueden desprenderse del informe realizado por la ONG ADC, titulado “*#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires*” (Ucciferri, 2019).

De allí se desprende que el sistema será utilizado «únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC)».

Según el GCBA «los archivos que se generan se encuentran en poder de la autoridad policial y su tratamiento queda sujeto a sus protocolos de seguridad, privacidad y confidencialidad, encontrándose prohibida su cesión a ninguna otra autoridad administrativa de la CABA».

Como parte de la problemática planteada en la captura de video, tenemos una regulación débil en muchos casos, tal como se describe en el trabajo de investigación presentado en el congreso de informática bajo el título “*Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales*” (Cejas & González, 2015).

A lo antes expuesto, se puede hacer mención también a antecedentes como el de la ciudad de San Francisco (Estados Unidos), ciudad que prohibió el uso de cámaras con reconocimiento facial en mayo de 2019.

“Ahora podrían seguirla en un futuro cercano la vecina Oakland, que está considerando una prohibición similar, y el estado de Massachusetts, donde el Senado estatal también estudia la cuestión. ... los grupos en defensa de los derechos civiles aseguran que esta tecnología invade la privacidad de los ciudadanos de forma excesiva...”

tal como se desprende del artículo periodístico (ABC - San Francisco, reconocimiento facial, 2019).

Sin duda en mi rol de ciudadano, estoy de acuerdo en todas las medidas que se puedan llegar a tomar para mejorar las condiciones relacionadas a la seguridad (o mejor dicho a la falta de ella), sin embargo, considero que el fin no justifica los medios, y que varios aspectos relacionados con la temática se deben al menos un debate público. A decir:

- Almacenamiento de las imágenes. Seguridad y protección de copias de seguridad, tiempo de conservación.

- Posibilidades que tienen los operadores de los sistemas de manipular la información visualizada/almacenada. Convenios de confidencialidad que los alcanza.

El acceso a las imágenes, permite en poco tiempo y con alta precisión conocer los hábitos de vida de los ciudadanos. La práctica de instalación de cámaras que graben todo el movimiento de los ciudadanos, no sólo se da en la vía pública, también por ejemplo en el transporte público de pasajeros, las estaciones de peaje y hasta en escuelas. A esto hay que sumar las instaladas por vecinos en muchos casos enfocando a las veredas, para poder captar los ingresos a sus viviendas, empresas, comercios. Todo esto sin mucho o ningún control, en pos de mejorar la seguridad de todos. Creo que es hora de poner el tema sobre la mesa, incentivar al debate y pensar al respecto. ¿Está bien llenar la ciudad de cámaras? ¿Es correcto? ¿Afecta mi privacidad? ¿Viola mis derechos?

### **Hackers**

Son aquellas personas que se encuentran constantemente intentando ganar acceso a dispositivos e información con algún tipo de valor. Como se mencionó con anterioridad, probablemente podríamos llegar a pensar que no tenemos información con el suficiente valor como para que el esfuerzo de una persona para robarla valga la pena. Sin embargo, al pensar en nuestra información financiera, nuestras claves importantes (correo electrónico, redes sociales, home banking) seguramente imaginemos la importancia que la misma tiene, para nosotros. Pero ¿para un hacker?

Invito al lector a pensar si por el accionar de un hacker, todas nuestras fotos familiares en formato digital, nuestros documentos personales y/o laborales, así como otros archivos de relevancia (por no decir, todo el contenido almacenado en nuestros dispositivos) fuera cifrado, y por lo tanto perdiéramos el acceso al mismo. Salvo claro, pagando una suma de dinero a través de una transferencia bancaria, bitcoins o algún otro medio facilitado por los “secuestradores”. Sin duda es lo más parecido a un secuestro. No físico (pues los bienes físicos no son sustraídos, si a nivel de software), no virtual (pues el hecho se consume en sí mismo) pero no hay margen de duda de la gran relevancia de los bienes a los que dejamos de tener acceso. En muchos casos, el trabajo de días, meses, años, de una vida (no ahondaremos en la importancia de contar con copias de seguridad de nuestra información de relevancia) podría llegar a perderse. Lo que para muchos lectores podría parecer algo de película, algo raro, sucede y mucho y a cualquier usuario, independientemente de la relevancia que a priori pueda contener la información almacenada en sus discos duros.

Esto es algo muy usual el día de hoy. Los productos de software malicioso que realizan estas prácticas son conocidos como ransomware. Algo similar sucede actualmente con el robo de material sensible desde dispositivos, con el posterior pedido de “rescate” para evitar la divulgación de dicho material. Hemos sido testigos de innumerables casos de robo de fotos privadas con contenido erótico de artistas, los cuales fueron extorsionados para hacer un depósito de dinero para evitar que las mismas salieran a la luz. Sin duda, un clarísimo ejemplo de violación a la privacidad.

Otros ejemplos podrían ser los conocidos como robo de identidad, a través de los cuales, un hacker o una persona con fines maliciosos, podría hacerse pasar por nosotros, empleando las credenciales de acceso a una red social, y publicando contenido como si fuéramos nosotros. O lo que podría ser más grave aún, el robo de claves de acceso a tarjetas de crédito, con el posterior uso del crédito ajeno para hacer compras u otros gastos. Los ejemplos son innumerables, y lo “bueno” del caso, es que se trata de todos ejemplos tangibles, que en el día a día nos hacen sencillo imaginar su ocurrencia y hasta algunas de sus consecuencias.

Más ejemplos de este estilo sobran:

- Phishing: método a través del cual se nos invita a ingresar a una página web que simula ser del banco, o del correo electrónico o de otros sitios que solemos usar, con el fin de robarnos usuarios y claves.
- Los conocidos métodos empleados en los cajeros automáticos para robarnos las tarjetas de débito y hacernos ingresar en una falsa mesa de ayuda para que ingresemos nuestra clave.
- Y cientos de mecanismos de “cuentos del tío” que se van perfeccionando con increíble imaginación.

## **Gobierno**

Quizás esto suene a película de espías norteamericanos contra los rusos, de agentes secretos, James Bond (agente 007), “Misión Imposible”, por qué no el Súper agente 86 o cualquier otra del estilo. Sin embargo, quizás no sea tan tangible en Argentina o quizás no al nivel de superproducción de Hollywood, porque en Argentina también tenemos lo nuestro. Cabe citar el caso mediático con Jaime Stiuso como protagonista. Ex espía/agente de inteligencia argentino (Secretaría de Inteligencia, anteriormente SIDE), del cual pesan acusaciones cruzadas de escuchas telefónicas. Pero sin duda el “espionaje” de los ciudadanos a través de internet es una práctica que existe y que muchos gobiernos no pueden negar. En muchos casos los gobiernos buscan conocer qué piensan los ciudadanos, qué problemáticas tienen, y bajo el lema de la

“información es poder” suelen valerse de cualquier medio para hacerse de la misma. Para tangibilizar esto y conocer un poco el alcance cabe citar algunos ejemplos:

- Estados Unidos post derrumbe de las torres gemelas en el año 2001, con el patriotismo de los ciudadanos herido, y con la premisa de combatir el terrorismo, dio luz verde para permitir a sus organismos de inteligencia a interceptar cualquier tipo de comunicación entre cualquier persona, con el fin de poder dar con potenciales negociaciones terroristas. Algunos de los sistemas informáticos empleados para tal fin, fueron Echelon y Carnivore.
- En el año 2010, con la figura de Julian Assange y el famoso WikiLeaks se hicieron públicos una enorme cantidad de documentos confidenciales que, entre otras cosas, comprometieron a varios gobiernos por el ejercicio de prácticas relacionadas a la captura de información de las personas.
- En el año 2013, a través del estadounidense Edward Snowden, ex empleado de la CIA (Agencia Central de Inteligencia de Estados Unidos) y de la NSA (Agencia de Seguridad Nacional de Estados Unidos) se dejó al descubierto la forma en que Estados Unidos con sus aliados, vigilaba (ó vigila) a través de sus agencias de inteligencia a la población mundial. Se brinda un mayor detalle sobre este escandaloso acontecimiento en la sección “Hechos que vale la pena conocer”- “Los ciudadanos del mundo bajo vigilancia” en el CAPÍTULO III de este documento.
- En países no democráticos en los que prevalece un régimen autoritario, estas prácticas son mucho más visibles.

### **Proveedores de Servicio de Internet (ISPs)**

Las compañías que proveen el servicio de internet, obviamente realizan un monitoreo del uso que sus usuarios realizan de dicho servicio. Por un lado, como forma de evaluar si el servicio prestado es de buena calidad, pero por otro lado, esta información es sin duda una fuente inagotable de conclusiones, de estadísticas, de conocimiento sobre los hábitos de las personas, sus necesidades, sus reclamos, sus descontentos, sus estados de ánimo.

Sin ir más lejos, en marzo de 2017, Estados Unidos votó a favor de la revocación de una ley (promulgada por Barack Obama) a través de la cual, se evitaba que los ISPs pudieran “compartir/comercializar” la información recolectada de sus usuarios, sin su previo consentimiento.

A partir de la nueva ley del gobierno de Donald Trump, se habilita a las compañías proveedoras de servicio de internet, a comercializar todo tipo de datos de los internautas como ser historial de navegación, su localización, registro aplicaciones empleadas, tipo y característica del dispositivo empleado para conectarse a la red. Esta información es oro para empresas anunciantes que deseen información de los potenciales consumidores.

Esta nueva legislación, divide las aguas en Estados Unidos ya que mucha gente la ve como una violación a los derechos de privacidad de los internautas.

“La nueva directriz permite a las empresas de telecomunicaciones vender todo tipo de datos de los internautas, desde su historial de navegación, hasta su localización, el registro del uso de aplicaciones o el tipo de dispositivo desde el que usan la red, entre otros.

Compañías como Verizon, AT&T o Comcast podrán a partir de ahora comercializar con la información privada de sus clientes a su entera discreción y vender esos datos a anunciantes.”

(BBC - ISPs en EEUU, 2017)

Si deseáramos orientar algún tipo de publicidad comercial o política, sin lugar a duda toda esta información nos daría una enorme ayuda, ¿no lo creen?

A modo de resumen de lo expuesto en este apartado, se presenta el Gráfico 4.



Gráfico 4: Qué proteger y de quién.

## CAPÍTULO III: El Mundo digital.

La revolución tecnológica ha empezado hace tiempo, y no piensa detenerse. Muy por el contrario, los países que no inviertan en tecnología verán con el transcurrir de los años, un impacto negativo en su economía. En todos lados empieza a leerse sobre las profesiones del futuro que aún no existen, y que serán indispensables para cubrir las nuevas necesidades que la evolución tecnológica empieza a introducir en todo el mundo. Mucha de esta evolución, también puede medirse en la cantidad de dispositivos que se suman a la red año tras año, así como también la cantidad de personas que se suman como internautas, y a su vez el volumen de datos, información, transacciones online que crece año tras año.

En este apartado, se presentan al lector datos relacionados con este crecimiento con números que permiten dimensionar de qué se trata.

### Penetración digital en el mundo

Este párrafo tiene por intención mostrar a través de gráficos y estadísticas, el nivel de penetración que la tecnología está logrando a nivel mundial, y cómo la misma se arraiga año tras año. Varios de los gráficos aquí expuestos, forman parte del reporte trimestral correspondiente al tercer trimestre elaborado en el mes de julio de 2019 por Hootsuite y WeAreSocial (Global Digital - Julio 2019, 2019), del mismo reporte pero elaborado en enero de 2019 (Global Digital - Enero 2019, 2019), y del elaborado en octubre de 2019 (Global Digital - Octubre 2019, 2019).



Gráfico 5:

“Digitalidad” en el mundo.

Algunos números de relevancia para el análisis del tema. Con una población de 7.734 millones (o 7,734 billones en la

nomenclatura americana) de los cuales el 55% está urbanizada. Las cantidades de: usuarios de teléfono celular es de 5.155 millones (67% de la población mundial); usuarios de internet es de

4.479 millones (58% de la población mundial); usuarios activos de redes sociales es de 3.725 millones (48% de la población mundial); usuarios de redes sociales a través de dispositivos móviles es de 3.660 millones (47% de la población mundial).



Gráfico 6: Crecimiento digital anual. Evolución interanual de la “digitalización” del mundo. Nótese que todos los indicadores

referentes al crecimiento en el uso de la tecnología (2do al 5to) se han incrementado por encima del crecimiento poblacional. Entre octubre 2018 y octubre 2019: la población mundial creció 1% (79 millones más); la cantidad de usuarios de dispositivos móviles creció 2,4% (123 millones más); la cantidad de usuarios de internet creció 10% (416 millones más); la cantidad de usuarios activos de redes sociales creció 9,6% (328 millones más) y la cantidad de usuarios de redes sociales a través de dispositivos móviles creció 15% (476 millones más).

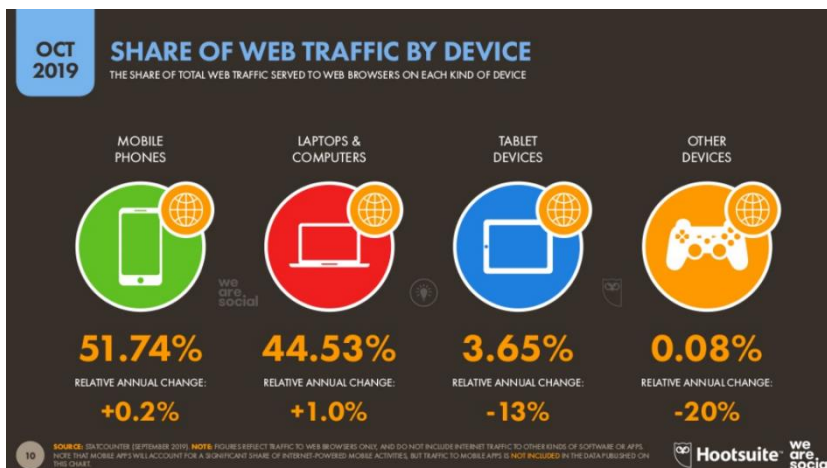


Gráfico 7: Tráfico de internet por dispositivo. Nótese el desplazamiento de la computadora y laptops en manos de los teléfonos móviles. El tráfico

en internet generado por: teléfonos móviles, representa el 51,74% (sólo 0,2% más que el año pasado); laptops y computadoras, representa el 44,53% (1% más que el año pasado);

tablets, representa el 3,65% (13% menos que el año pasado); otros dispositivos, representa el 0,08% (20% menos que el año pasado).

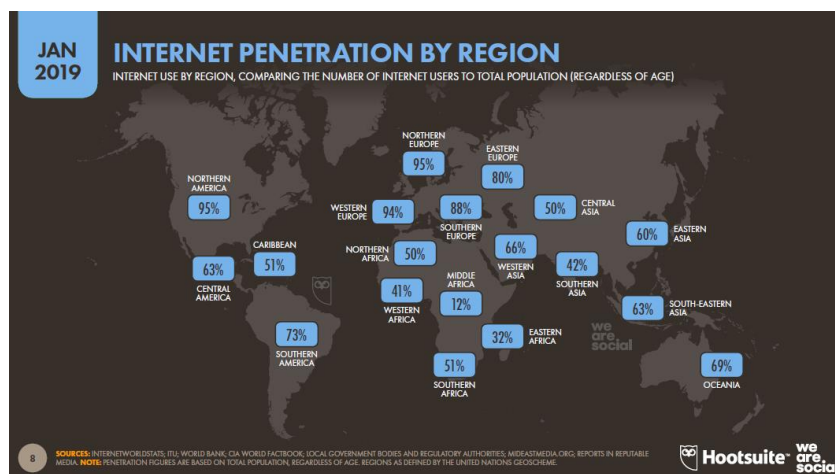


Gráfico 8:  
Penetración de internet por región. Proporción entre cantidad de usuarios de internet, con la población total de cada región (sin tener en cuenta la edad).

## Penetración digital en Argentina

El siguiente apartado pone en foco el nivel de penetración que la tecnología tiene, pero ahora en nuestro país. Los gráficos expuestos, forman parte del reporte elaborado el 31 de enero de 2019 por Hootsuite y WeAreSocial para Argentina (Digital 2019 en Argentina , 2019).

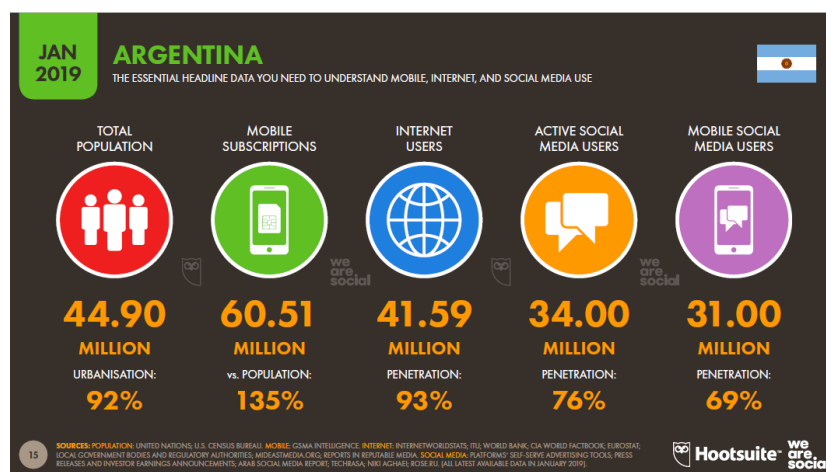


Gráfico 9:  
Principales datos sobre móviles, internet y uso de redes sociales en Argentina.



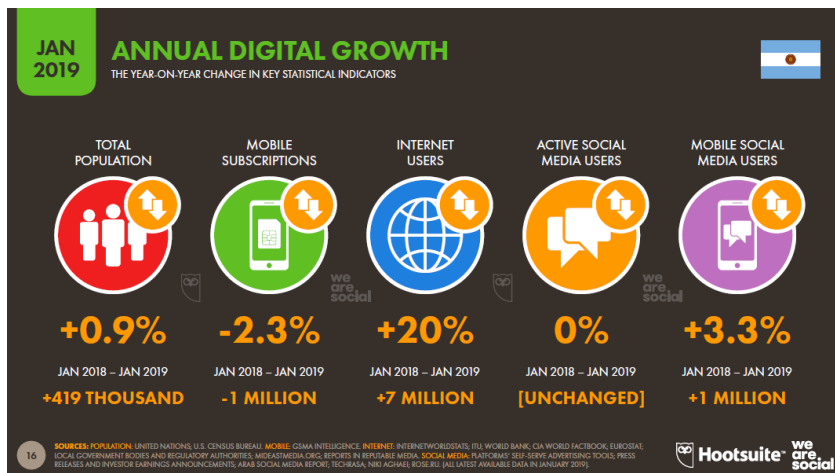


Gráfico 10: Crecimiento digital anual en Argentina. Evolución interanual en indicadores clave. Notar la disminución de las

suscripciones a telefonía móvil (-2,3%) que podría explicarse por la recesión y la crisis económica, y el gran crecimiento de la cantidad de usuarios de internet (+20%).

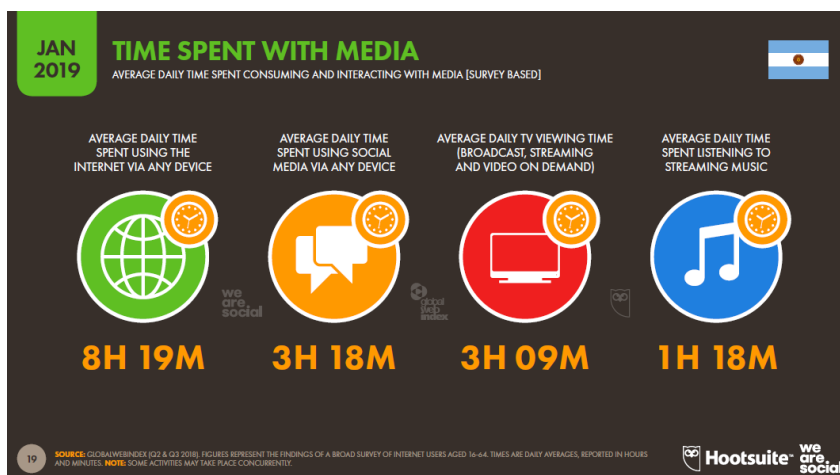


Gráfico 11: Tiempo empleado en medios (audio, video, internet en general, redes sociales, streaming) en Argentina. Promedio del

tiempo diario que los argentinos emplean en cada tipo de actividad relacionada a los medios. Podría calificarse como tiempos prolongados.

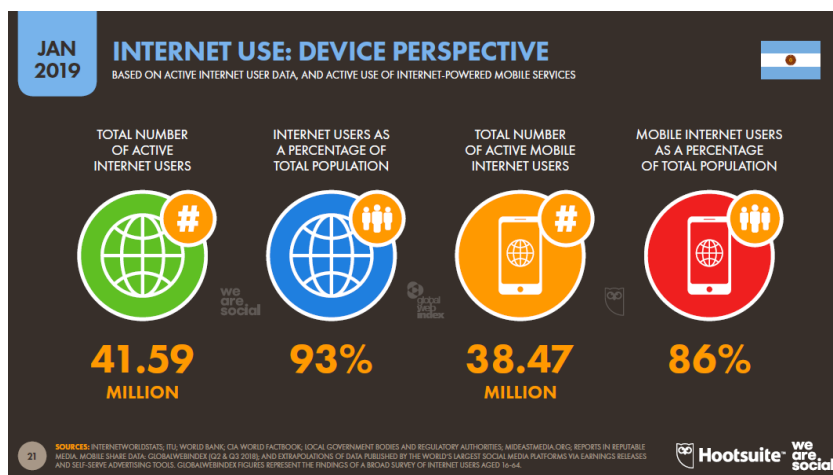


Gráfico 12: Uso de Internet (en Argentina): Perspectiva del dispositivo.

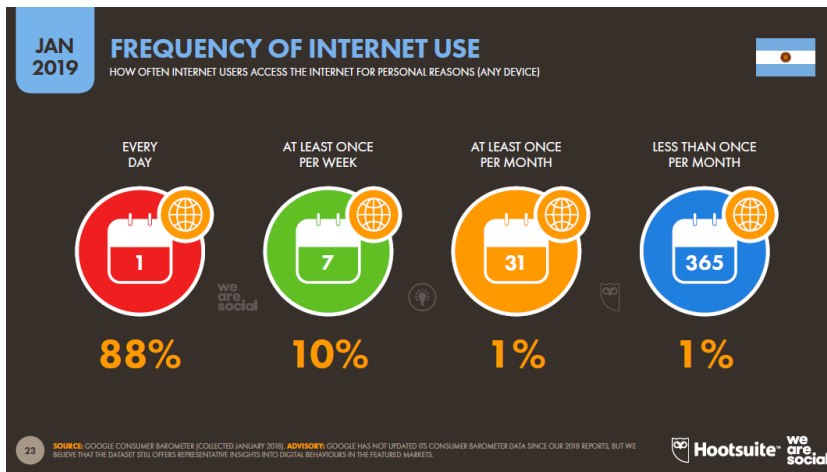


Gráfico 13:  
Frecuencia en el uso de Internet en Argentina. Con cuánta frecuencia los usuarios acceden a internet por razones personales

(independientemente del dispositivo empleado).

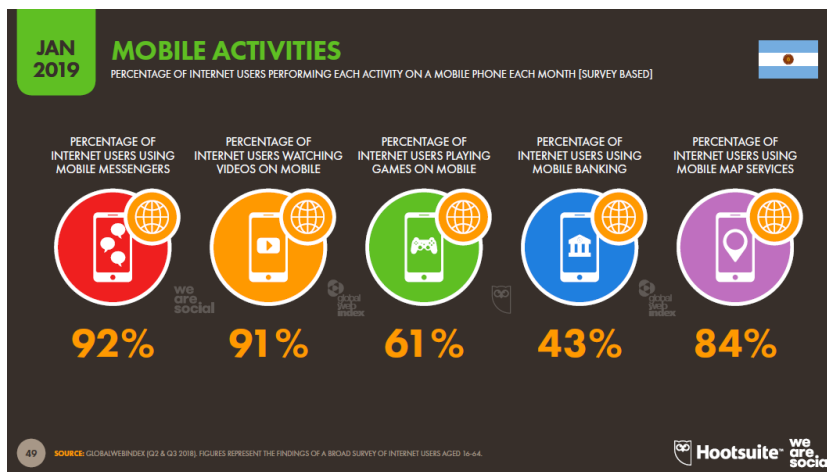


Gráfico 14:  
Actividades móviles en Argentina. Porcentaje de usuarios de internet que realizan cada actividad empleando un

teléfono celular de manera mensual.

### Un minuto en internet.

En esta sección se presenta información de acuerdo al reporte anual correspondiente al año 2019 de la empresa Domo (Data Never Sleeps 7.0 en Domo), en el cual se ilustra la cantidad de transacciones asociadas a la actividad del mundo en internet, que suceden en el transcurso de un minuto. Es interesante visualizar el volumen de información que se genera, y cuánto a su vez se puede “aprender” de la misma tal como se trata a lo largo de este documento.

Qué sucede en un minuto en el 2019:

- Sólo en Estados Unidos, se usan alrededor de 4.416.000 gigabytes de datos de Internet. 41% más que en 2018.
- Se publican 511.200 Tweets en todo el mundo.

- Se publican 55.140 fotos en Instagram. 12% más que en 2018, donde se publicaron 49.380 imágenes por minuto en Instagram.
- 231.840 llamadas son realizadas empleando Skype.
- Se transmiten 694.444 horas de contenido en Netflix.
- 4.500.000 videos se reproducen en YouTube. Mientras que en el 2018, las reproducciones por minuto eran 4.333.560.
- Se reservan más de 9.772 viajes en Uber, lo que implica un aumento del 603% respecto al 2018.
- Se realizan 1.389 reservas a través de Airbnb.
- Google procesa casi 4.500.000 búsquedas.
- Se envían más de 18 millones de mensajes de texto.
- Se envían casi 188 millones de correos electrónicos (caída del 8% desde el año 2014).
- Se descargan más de 390.000 aplicaciones.

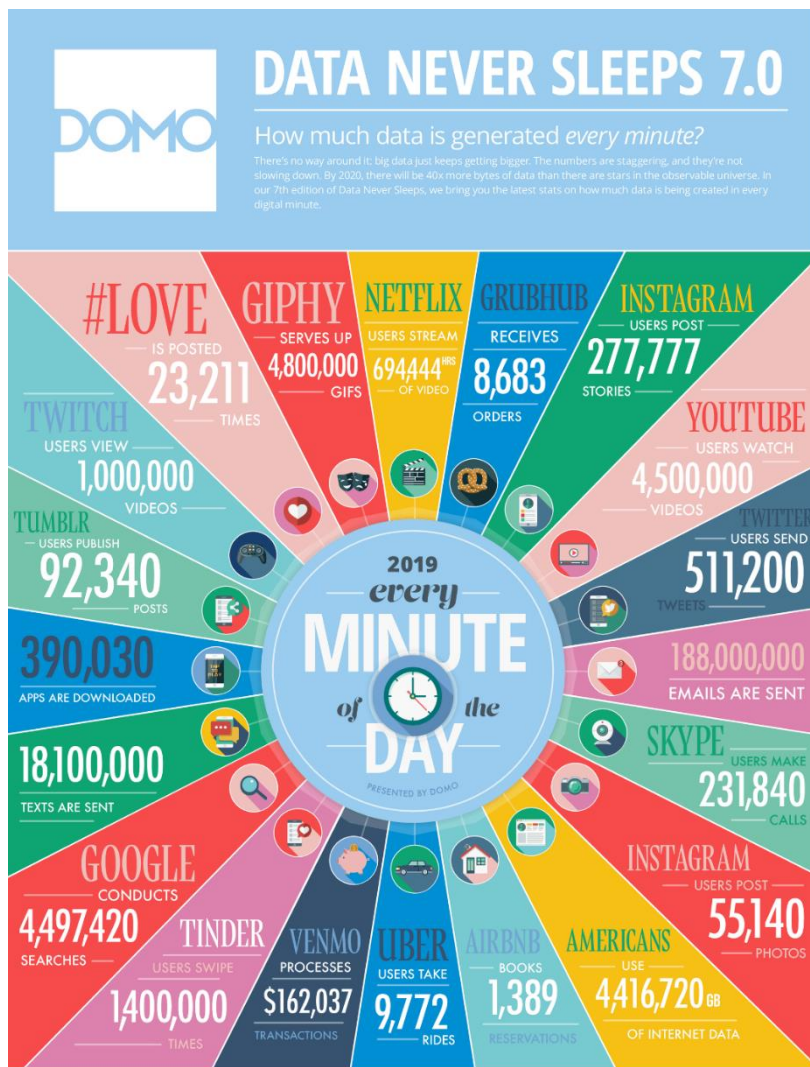


Gráfico 15: ¿Qué pasa durante un minuto en Internet?

## Redes sociales

Tal como pudiera observarse a través de las estadísticas relacionadas a la penetración digital tanto en nuestro país como en el mundo, las redes sociales son sin duda grandes protagonistas en esta carrera de juntar usuarios, conectar realidades, y en el contexto que nos interesa abordar en el presente documento de investigación, recolectar información. Este apartado tiene como finalidad, introducir de manera más detallada al lector en este impresionante mundo de las redes sociales analizando estadísticas más precisas que abrumen, relacionadas al uso de las mismas tanto a nivel mundial, como en particular en nuestro país. Estadísticas que nos permiten enmarcar a nuestro país en el mapa de países con un elevado nivel de uso en dicha tecnología. Tal como conocemos la tecnología relacionada con las redes sociales, que es el concepto que nos interesa abordar en esta investigación, y tomando la definición de la Real Academia Española (RAE) (RAE - Red Social):

“Servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base a criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo.”

## Números en el mundo

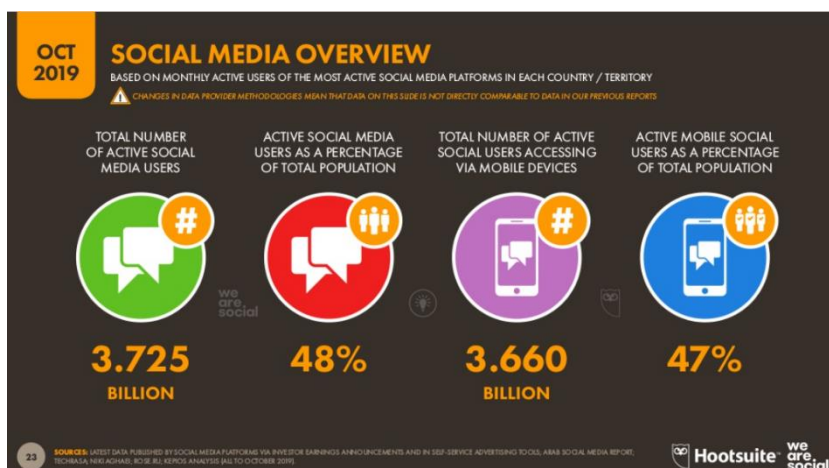
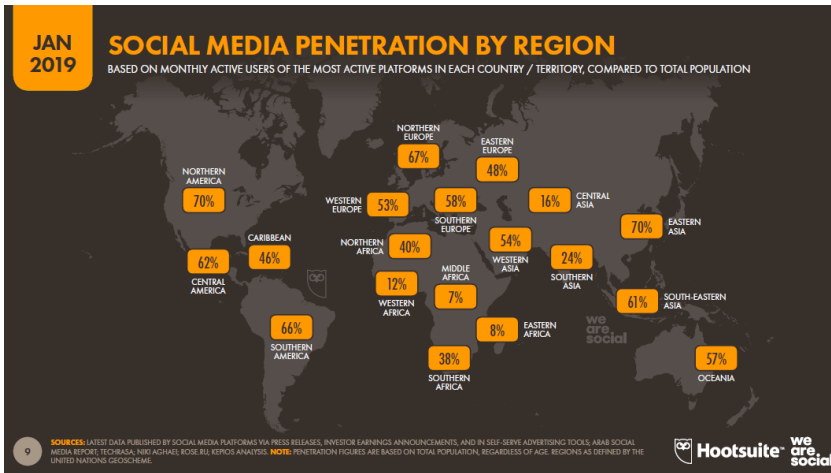


Gráfico 16: Visión general de las redes sociales.

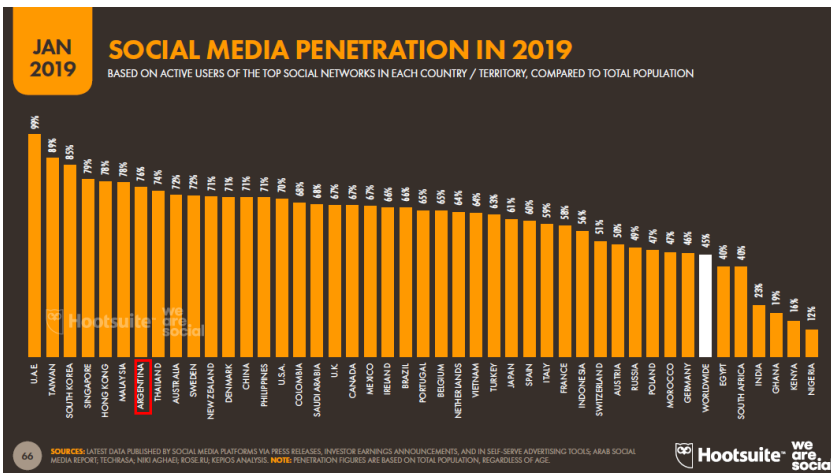
Basado en usuarios activos de las redes sociales más empleadas en cada país o territorio. La cantidad de usuarios

activos de redes sociales es de 3.725 millones (48% de la población mundial). Se debe tener en cuenta que no son personas únicas, ya que una misma persona tiene más de un usuario (entre 5 y 9 dependiendo la edad, de acuerdo al Gráfico 96).



comparado con los totales poblacionales.

Gráfico 17:  
Penetración de las redes sociales por región. Basado en usuarios activos de las redes sociales más empleadas en cada país o territorio



comparado con los totales poblacionales. Podemos encontrar a nuestro país entre los países con mayor penetración, con un 76%, muy por encima del 45% del promedio mundial.

Gráfico 18:  
Penetración de las redes sociales en 2019. Basado en usuarios activos de las redes sociales más empleadas en cada país o territorio

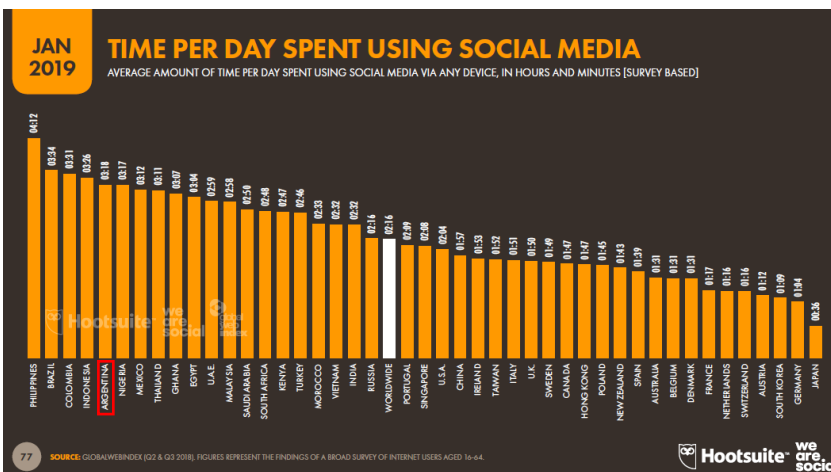


Gráfico 19: Tiempo por día dedicado a las redes sociales. Vía cualquier dispositivo. Medido en horas y minutos. En Argentina cada persona emplea 3 horas 18 minutos

por día en redes sociales, y se encuentra muy por encima del promedio mundial (2 horas 16 minutos)

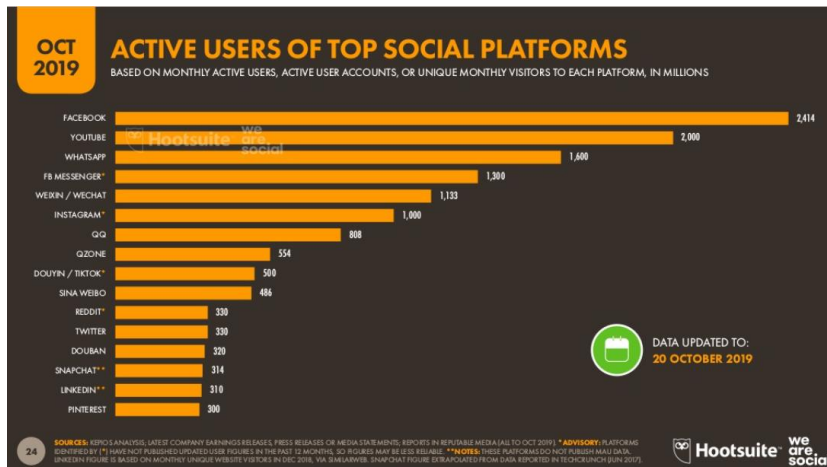


Gráfico 20:  
Usuarios activos en las principales redes sociales.

De las imágenes expuestas con anterioridad junto con aquellas disponibles en el ANEXO I de este documento (en el cual el lector puede encontrar más estadísticas relacionadas), son varias las conclusiones que se pueden extraer. En general, todas hacen referencia a una gran penetración del fenómeno de las redes sociales en nuestro país. A decir:

- En el Ranking mundial de “penetración elegible” de las redes sociales Argentina se ubica en la posición 17 (Gráfico 95).
- En lo que respecta al tiempo empleado por día por cada usuario en la red, Argentina se encuentra en la 5ta posición a nivel mundial, con un tiempo que podría considerarse como muy alto, y muy por encima del promedio (Gráfico 19).
- La cantidad promedio de cuentas de usuarios de redes sociales por persona, es de 9 (Gráfico 96).
- El ranking de los países con las más grandes audiencias para publicitar a través de Facebook) ubica a Argentina en el puesto 17 (Gráfico 100), con un alto porcentaje de usuarios mayores de 13 años. El mismo ranking, pero para Instagram lo coloca en la posición 13 (Gráfico 105) y para Twitter en la posición 17 (Gráfico 106).
- El ranking de porcentajes de alcance elegible en Facebook ubica a Argentina en el puesto 20 a nivel mundial (Gráfico 101), con un alto número de usuarios alcanzables.
- La media mensual de clics por usuario en anuncios de Facebook es de 11, contra un promedio mundial de 8 (Gráfico 104).

Son todos datos que hablan a las claras que Argentina es un mercado por demás apetecible para las redes sociales. Los usuarios argentinos, usan muchas redes sociales, mucho tiempo,

y se puede llegar a ellos a través de dicha tecnología de manera muy extensa. Por lo cual, contar con herramientas que le permitan conocer los riesgos que acarrea el uso de las mismas, es un punto de vital relevancia para protegerse.

De todo lo antes mencionado, se desprende la necesidad de concientizar a los usuarios argentinos de redes sociales (y de TICs en general), de manera tal otorgarles las herramientas para que puedan hacer un uso seguro de la tecnología.

## Números en Argentina

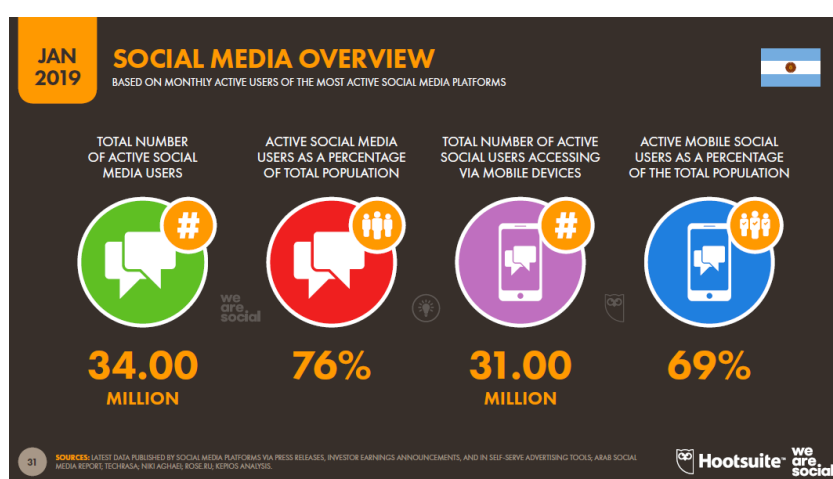


Gráfico 21: Visión general de las redes sociales en Argentina.

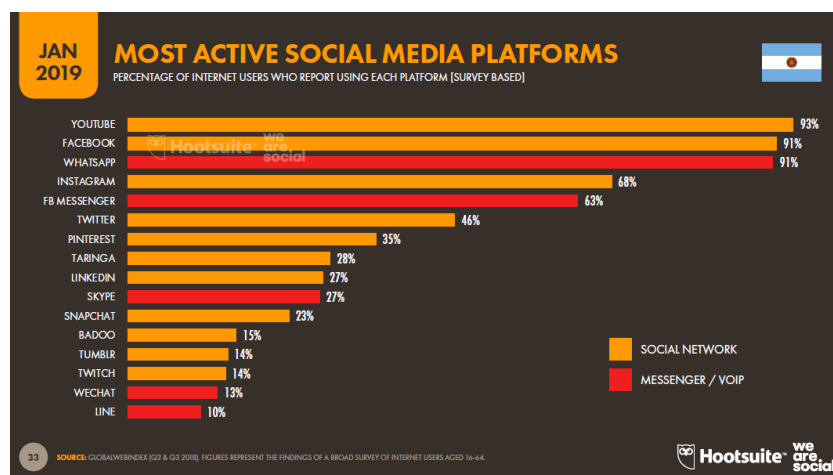


Gráfico 22: Plataformas de redes sociales más activas en Argentina.

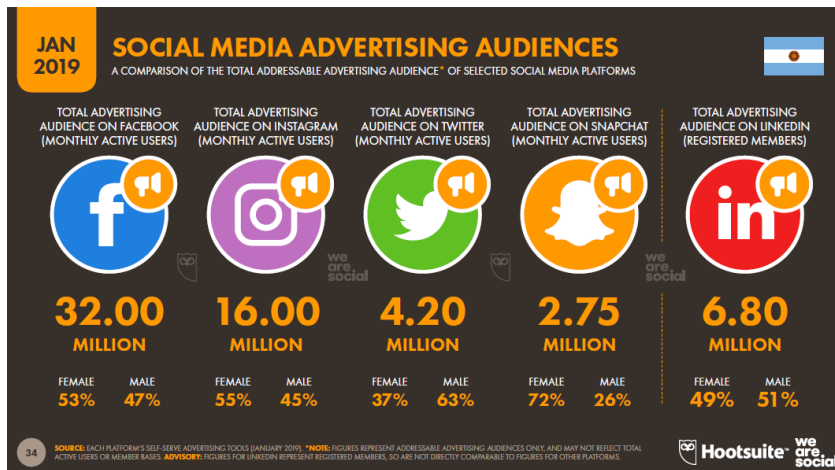


Gráfico 23: Audiencia sobre la cual se podría publicar en redes sociales en Argentina. Comparación de la totalidad de la audiencia sobre la

cual se podría publicar en redes sociales seleccionadas.

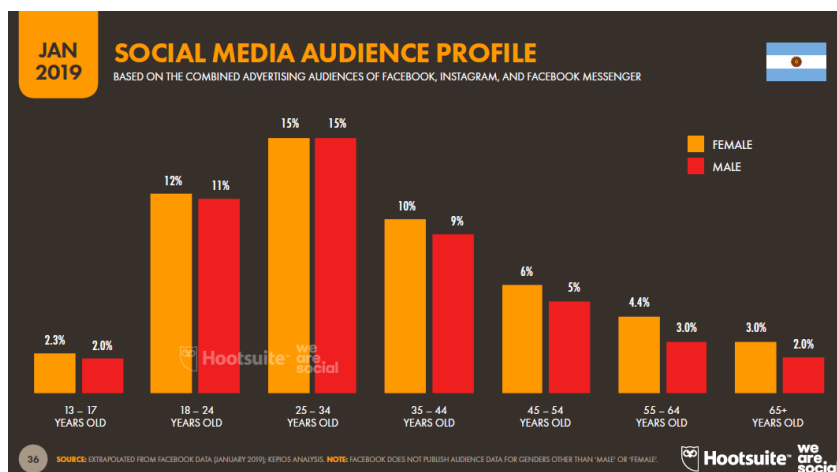


Gráfico 24: Perfil de la audiencia sobre las cuales se podría publicar en Argentina. Basado en la audiencia de Facebook, Instagram y

Facebook Messenger combinadas. Porcentaje de cada tipo de perfil, tipificado por rango etario, y género.

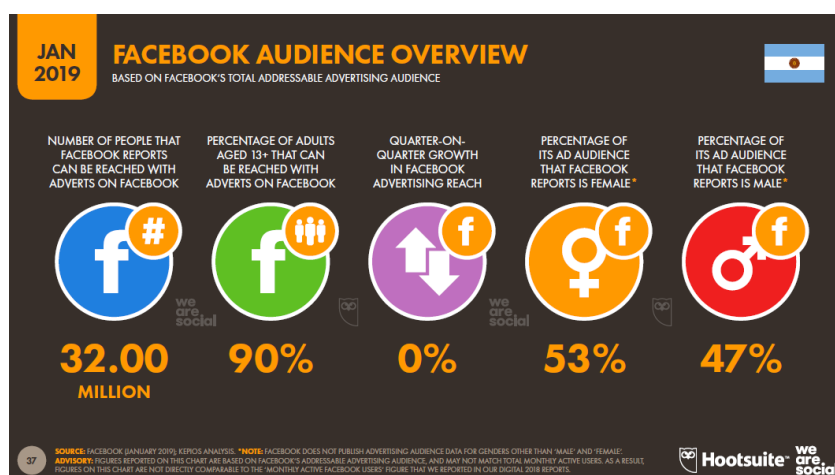


Gráfico 25: Visión general de la audiencia de Facebook en Argentina. Basado en el total de la audiencia sobre la cual se podría publicar

en Facebook en Argentina.



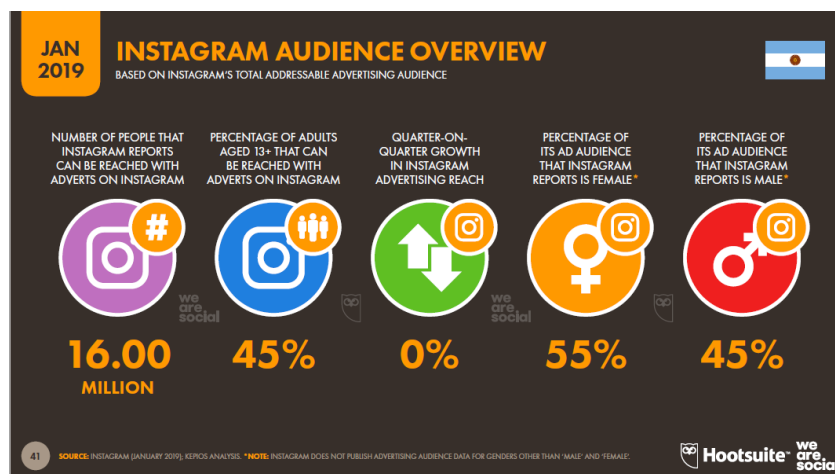


Gráfico 26: Visión general de la audiencia de Instagram en Argentina. Basado en el total de la audiencia sobre la cual se podría publicar

en Instagram en Argentina

No hay manera de discutir el nivel de penetración de las redes sociales. Su uso es intensivo en casi todo el mundo, exceptuando países en los que su uso tiene algún tipo de prohibición de los cuales se hace mención en el apartado “Censura digital en el mundo” del CAPÍTULO IV de este documento.

Basta con ver las cantidades de usuarios activos por mes que manejan las redes sociales (Gráfico 20), para imaginar el enorme y apetecible negocio que se esconde atrás de cada uno de esos potenciales consumidores.

No es casualidad que para hacer uso de estas redes, no sea necesario desembolsar un solo peso de nuestro bolsillo. Que lo único que hace falta, es introducir algunos datos verificables, que son los que conformarán nuestro “perfil” en la red tales como una dirección de correo electrónico verificable, nombre y apellido, fecha de nacimiento, dirección de residencia. Algunas redes podrán indagar sobre nuestros hábitos de consumo, lugares frecuentados entre otros muchos datos. Toda información que a priori, podríamos imaginar que tiene poco o nulo valor para cualquier otra persona que no seamos nosotros. Primer gran equivocación.

Hay una frase en el mundo de los servicios online, que sintetiza en pocas palabras cuál es el interés de estos sitios:

*“Si no estás pagando por el servicio, entonces tú eres el producto, no el usuario.”*

¿Cómo es esto? ¿Cuál es el negocio de estas redes?

El negocio consiste en almacenar toda la información posible sobre cada uno de los usuarios, de manera tal de armar un perfil, no sólo para la red social en sí, sino además un perfil como consumidor, como ciudadano, como persona. Toda esta información luego es vendida a otras empresas, y será de gran relevancia a la hora de convencernos en qué o en dónde podríamos

gastar nuestro dinero, o en qué servicios podríamos estar interesados, o en su defecto les facilitará el camino para obtener aún más información en caso de así desearlo.

Es impensada la cantidad de información que en general los productos de software que las personas emplean en su vida diaria, pueden obtener de ellos, y la manera en que la misma puede ser manipulada, para hacerse con ganancias incalculables. Si aún no queda claro la manera en que esto funciona, sólo basta con citar algunos ejemplos que sin duda a la mayoría de los lectores les habrá llamado la atención en alguna oportunidad.

¿Será casualidad que luego de una simple búsqueda a través de google (o cualquier otro buscador), seamos “invadidos” por publicidad con estrecha relación con la búsqueda previamente realizada o con gran afinidad a características personales tales como edad, comidas preferidas, historia médica, fecha de cumpleaños, sitios web preferidos e infinidad de etcéteras? (Incluso, información tal como nuestras afinidades políticas, o ciertos detalles étnicos podrían formar parte de nuestro perfil, y podrían ser empleados para el direccionamiento de contenido) ¿Que luego nuestra cuenta de correo reciba correos con publicidades acordes a la temática? Además de ello, en algunos casos, las empresas podrían ser notificadas vía bluetooth o vía GPS, al momento en que pasamos y/o entramos a alguna de sus tiendas, así como también el tiempo que permanecemos comprando dentro de ellas. Tener un smartphone, es como tener un dispositivo de tracking continuo.

Al momento de crear nuestra cuenta por primera vez en las redes de estas características, o bien al momento de instalar la aplicación para nuestra PC, o teléfono móvil, seguramente hemos tenido que pasar por un paso que consiste en “Aceptar los términos y condiciones”. La pregunta de rigor para el lector es, ¿alguna vez se ha tomado el tiempo para leer de manera rigurosa y completa dichos términos y condiciones? ¿Ha tratado de entender de qué se tratan esos términos y condiciones? Lo ideal sería que si, pues es nada más y nada menos el “contrato” que estamos firmando con la red social, a través del cual se reglamenta el uso de la misma. Qué de nuestro contenido será realmente nuestro, y qué cosas estaremos “cediendo” a la red.

### **Condiciones de Servicio: El ejemplo Facebook**

En este apartado, nos tomaremos un tiempo para analizar de qué se tratan las condiciones de servicio de la red social que más usuarios activos posee, y sobre la cual tantos inconvenientes a nivel mundial hubo como consecuencia de manipulaciones quizás no del todo éticas (aunque si aparentemente legales) de la información de sus usuarios. ¿Y por qué decimos que dicha manipulación no fue ilegal? Justamente, por las condiciones de servicio que antes de hacer uso

de la plataforma, el usuario acepta sin objetar ninguna de sus cláusulas. Aunque se tomara todo el tiempo del mundo en leerlas, analizarlas, interpretarlas, en la mayoría de los casos llegaríamos a un punto de dos caminos posibles:

- Luego de malgastar el tiempo tratando de interpretar las condiciones, nos resignamos a no formar parte de la red, y no las aceptamos.
- Cerramos los ojos y aceptamos las condiciones, en pos de sumarnos al maravilloso mundo ofrecido por la plataforma (con todo lo que eso conlleva). Esto es lo que han hecho los más de 2.414 millones de usuarios que tiene Facebook (Gráfico 20).

Vale la pena aclarar que las condiciones de servicio analizadas en este apartado, se encuentran vigentes desde el día 1 de agosto de 2019. Este análisis se realizó en primera instancia con condiciones de servicio que Facebook tenía publicadas como vigentes con anterioridad a dicha fecha. Es decir, que el mismo debió ser realizado nuevamente una vez publicada las nuevas condiciones. El cambio de vigencia en las condiciones de servicio, fue anunciado por la plataforma a través de una página como la que se ilustra a través del Gráfico 27.



Gráfico 27: Página de condiciones de Servicio de Facebook.

Otra cosa que vale aclarar es que si bien en este apartado se toma como referencia a Facebook (más de 2.414 millones de usuarios activos en todo el mundo al 15 de julio de 2019 según Gráfico 20) dentro de las condiciones de servicio analizadas se encuentran incluidas las condiciones de la red Instagram. Esto se debe a que Facebook desde abril del 2012 adquirió Instagram (más de

1.000 millones de usuarios activos en todo el mundo al 15 de julio de 2019 según Gráfico 20) por lo cual se podría decir que ambas redes sociales, y todo el contenido generado por los usuarios de estas dos grandes redes sociales, van “a parar a la misma bolsa”, y están alcanzados por las mismas condiciones de uso que aquí se analizan. Lo mismo sucede además con WhatsApp (más de 1.600 millones de usuario activos en todo el mundo al 15 de julio de 2019 según Gráfico 20) la cual también fue adquirida por Facebook en el año 2014.

El análisis se realiza sobre varios puntos de relevancia que se consideran son para tener en cuenta, con el fin de conocer un poco más en qué consiste el “contrato que firmamos” con Facebook al momento de aceptar las condiciones analizadas.

Las condiciones más relevantes para el análisis, están transcritas en el ANEXO II del presente documento. Las mismas, están estructuradas más o menos de la siguiente manera (sólo se transcriben los puntos de interés para el análisis):

**Condiciones de Servicio de Facebook** (Facebook - Condiciones de Servicio, 2018)

- 1- Los servicios que proporcionamos
- 2- Cómo se pagan nuestros servicios.
  - **Política de datos**, que debe ser aceptada para poder usar los productos.
- 3- Tus compromisos con Facebook y nuestra comunidad
  - 1. Quién puede usar Facebook
  - 2. Qué puedes hacer y qué puedes compartir y qué actividades puedes realizar en Facebook
  - 3. Los permisos que nos concedes
  - 4. Límites en cuanto al uso de la propiedad intelectual

El análisis se realiza sobre los puntos en color “negro” de los antes mencionados, deteniéndose en cada uno de ellos, transcribiendo de manera textual en muchos casos el contenido. La intención es evidenciar las cesiones que uno como usuario hace, entender a qué se compromete, y qué derechos cede al momento de aceptar dichas condiciones.

El punto 1 “Los servicios que proporcionamos” hace una descripción de los productos y servicios ofrecidos por la plataforma. Por lo cual, para la finalidad del análisis que se pretende realizar, no es de relevancia.

En el punto 2, y bajo el título “Cómo se pagan nuestros servicios” se puede encontrar lo que en la página se denomina como “Política de datos” (Facebook - Política de Datos, 2018). Entre las Políticas en cuestión, se pueden observar varios párrafos con descripción minuciosa de lo que

Facebook pretenderá de toda la información que los usuarios publiquen a través de su plataforma.

El análisis sobre las políticas de la red social Facebook es sólo a modo de ejemplo, y teniendo en cuenta que se trata de la red social que cuenta con más usuarios activos mensuales en el mundo. De todos modos, para el resto de las redes sociales, las condiciones de servicio que debe aceptar un usuario (o un producto) son de similares características que las aquí analizadas.

De dichas políticas, se destaca:

### **¿Qué información recopila Facebook?**

- Todo lo relacionado al contenido publicado, la ubicación de las fotos, la fecha en la que fueron tomadas, así como también los metadatos que la cámara incorpora en las mismas.
- En caso de aceptarlo (o de no negarlo), datos relacionados con creencias religiosas, ideología política, nuestra salud, origen étnico o racial, creencias filosóficas, etc.
- Información de la red de contactos. Contactos más frecuentados, la manera en la que interactuamos con ellos, libreta de direcciones del dispositivo empleado, registro de llamadas, SMSs, páginas visitadas, grupos con los que estamos conectados.
- La manera en como usamos los productos. Qué contenidos vemos, qué funciones empleamos, acciones realizadas, duración de las mismas.
- Toda la información relacionada a las transacciones realizadas. Compras, donaciones incluido el detalle del medio de pago empleado (tarjeta débito, crédito), detalle de la facturación, etc.
- Todo lo que otros usuarios proporcionan sobre nosotros. Comentarios sobre nuestro contenido, contenido en el que nos encontremos incluidos (fotos, videos, etc).
- Toda la información relacionada a los dispositivos empleados. Teléfonos, TVs, computadoras, tablets. La información relacionada con todos los atributos que nos imaginemos, es recopilada. Desde el detalle de la tecnología de los mismos, como sistema operativo instalado, versión de todos los productos de software instalado en los mismos, nivel de carga de batería, potencia de la señal, espacio de almacenamiento disponible, tipo de navegador, información suministrada por el GPS (nuestra ubicación), todo el detalle de la red WiFi desde la cual el dispositivo se conecta (velocidad, nombre de la red, proveedor de internet, número de teléfono, etc). Se debe tener en cuenta que Facebook conoce nuestra ubicación, incluso si no usamos el GPS. Nuestros dispositivos suministran la suficiente información como para que pueda concluir la misma, como ser

la dirección IP, la antena/celda de telefonía celular en la cual se conecta. Incluso nosotros mismos a través de la confirmación a la participación a eventos, le suministramos valiosa información acerca de nuestra ubicación.

- El detalle de las cookies que se encuentran almacenadas en nuestros dispositivos, de las cuales se podría llegar a obtener mucha información relacionada a nuestra privacidad, y a la manera en la que interactuamos con otros sitios.
- Detalles en la manera en cómo operamos con nuestros dispositivos. La manera en cómo movemos el mouse, si ponemos una ventana en primer plano, o colocamos otra en segundo plano.
- Facebook cuenta con innumerable cantidad de plugins para que otros sitios web los incorporen. Por ejemplo, los botones de “Me gusta” o el inicio de sesión a través de Facebook en distintos portales web. A través de estos, Facebook es informado de casi todo lo que realizamos en esos sitios (es decir, incluso estando desconectados de Facebook).

#### **¿Cómo usa Facebook con toda la información que recopila?**

- Personaliza sus productos en base a lo que sabe que nos gusta (teniendo en cuenta todo lo recopilado) así como también la publicidad que se nos envía. Esto le permite, entre otras cosas:
  - o Completar cierta información nuestra de manera automática, como por ejemplo, en un formulario de registro de otro producto.
  - o En base al conocimiento de nuestra ubicación actual, enviarnos publicidad de empresas que se encuentren cerca.
- Investigación y desarrollo de nuevos productos. En el apartado “Las TICs, y la democracia. El escándalo Cambridge Analytica”, dentro de la sección “Hechos que vale la pena conocer” en el CAPÍTULO III de este documento, se trata el gran robo y manipulación de información realizado con la excusa de llevar a cabo estudios con fines académicos. De esa manera, la empresa Cambridge Analytica se adueñó de información de más de 87 millones de usuarios de manera escandalosa.
- Reconocimiento facial. Facebook es capaz de reconocer a las personas desde el material subido.

#### **¿Cómo se comparte esa información?**

- *“... otras personas que usan Facebook e Instagram y nosotros podemos conceder acceso a información pública o enviar dicha información a cualquier persona, tanto dentro*

*como fuera de nuestros Productos, incluido en otros Productos de las empresas de Facebook, en resultados de búsqueda o por medio de herramientas y API..”*

- Cualquiera con quien hayamos compartido un contenido, podría a su vez compartirlo con terceros sin que nosotros lo sepamos, y sin que tengamos control alguno sobre ello.
- *“Cuando decides usar aplicaciones, sitios web u otros servicios de terceros que utilizan nuestros Productos o están integrados con ellos, estas plataformas pueden recibir información acerca de tus publicaciones o del contenido que compartes.”*
- Facebook tiene el derecho de compartir la información recopilada con sus socios externos.

#### **¿Qué permisos le concedemos a Facebook sobre la información que recopila?**

- *“cuando compartes, publicas o subes contenido que se encuentra protegido por derechos de propiedad intelectual (como fotos o videos) en nuestros Productos, o en relación con ellos, nos otorgas una licencia internacional, libre de regalías, sublicenciable, transferible y no exclusiva para alojar, usar, distribuir, modificar, publicar, copiar, mostrar o exhibir públicamente y traducir tu contenido, así como para crear trabajos derivados de él...”. “Esta licencia caduca cuando tu contenido se elimina de nuestros sistemas.”* Pero con una serie de excepciones que podrían hacer que de manera fáctica, se prolongue indefinidamente.
- *“Nos concedes permiso para usar tu nombre y foto del perfil e información sobre las acciones que realizas en Facebook junto a anuncios, ofertas y otro contenido patrocinado que mostramos en nuestros Productos, o en relación con ellos, sin que recibas compensación de ningún tipo.”*

Como podemos ver, Facebook no esconde nada en sus políticas. Todo está escrito ahí. Qué recopila, y hasta qué hace con toda esa información recopilada. Qué derechos cedemos sobre todo lo que hacemos o publicamos en lo que hace llamar sus “Productos”. Si algún lector desconocía esto, seguramente es porque nunca se ha tomado el tiempo de leer las complejas políticas de los servicios.

Cada mínimo detalle relacionado a cada pequeña acción que el usuario realiza, es registrada y almacenada. De hecho, mucha de esa información registrada, hasta podría parecer sin valor, o podríamos desconocer a priori, qué utilidad podría dársele a la misma.





Una de los grandes ganadores de la era de la recolección de la información de los internautas, es sin lugar a dudas Google. Se trata de una empresa visionaria que se inició con un simple buscador de contenidos en la web, gratuito, como resultado de un proyecto de dos estudiantes. El mismo podía ser usado por cualquier persona que lo deseara sin ningún costo para ello. Pero claro, todas las empresas requieren de dinero para subsistir, y obviamente Google no fue la excepción.

En el año 1999 Google lanza a la web la primera versión de su motor de búsqueda. Y desde ahí, ha tenido un crecimiento sostenido hasta llegar al gigante tecnológico que conocemos hoy.

A Google no le ha ido nada mal en los negocios. Sólo para tener una idea, a continuación mediante el Gráfico 29, se muestra la evolución de los ingresos anuales (Fernández, 2019):

### **Evolución de los ingresos de Google a nivel mundial desde 2002 hasta 2018 (en miles de millones de dólares)**

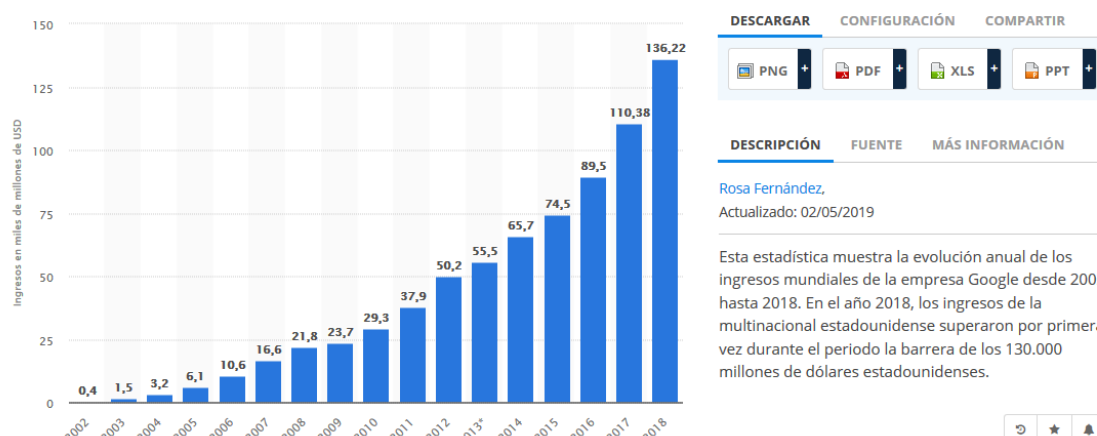


Gráfico 29: Evolución de las ganancias de Google.

En el año 2018, y según el Gráfico 29, las ganancias de Google fueron de 136.220 millones de dólares. Eso nos da unos 4.319,5 dólares por segundo. Nada mal. No hay mucho que aclarar del gráfico. Se ve claramente cómo desde el año 2002 al 2018, los ingresos sólo han crecido. Para analizar con más detalle la fuente de dichos ingresos, lo que permitirá también introducir al lector sobre el modelo de negocio de este gigante tecnológico, se presenta el Gráfico 30 extraído de una nota del diario BBC (¿Cómo hace Google para ganar tanto dinero? en BBC, 2016)

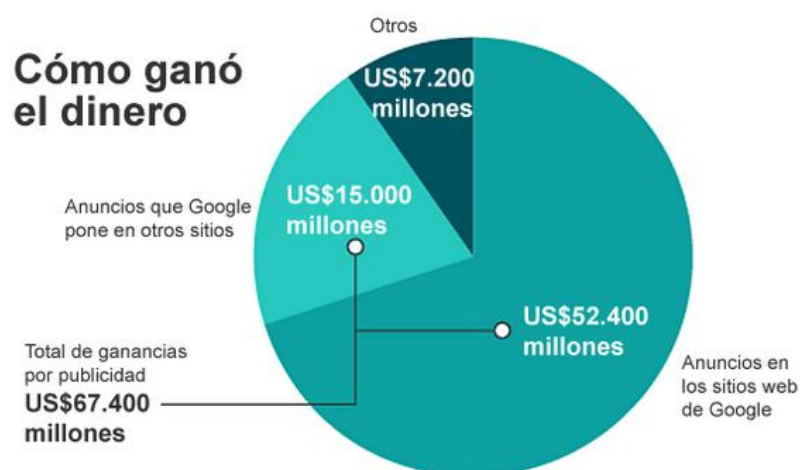


Gráfico 30: Distribución de las ganancias de Google.

Del gráfico anterior, se desprende que el máximo ingreso proviene de los anuncios. Y es en este campo en el cual Google ha sido un pionero en la manera de llegar a los consumidores.

La comodidad asociada con el uso de la tecnología no se puede negar, pero tampoco se puede ignorar su costo.

Invito al lector a que se detenga a pensar sobre la cantidad, tipo y calidad de información que de manera diaria ingresa en las aplicaciones de este gigante. Quizás antes de detenerse a pensar en ello, deba pensar en cuáles son las aplicaciones de uso diario que le pertenecen a Google, ya que con el correr de los años, son más y más las herramientas exitosas que son absorbidas por este gigante. Para tener un pantallazo, de cuántas y cuáles son las herramientas que forman parte de la enorme y completa suite de Google, a través de los gráficos Gráfico 31, Gráfico 32 y Gráfico 33 pueden observarse los íconos y nombres de esta impresionante batería de soluciones.

Productos para todos:

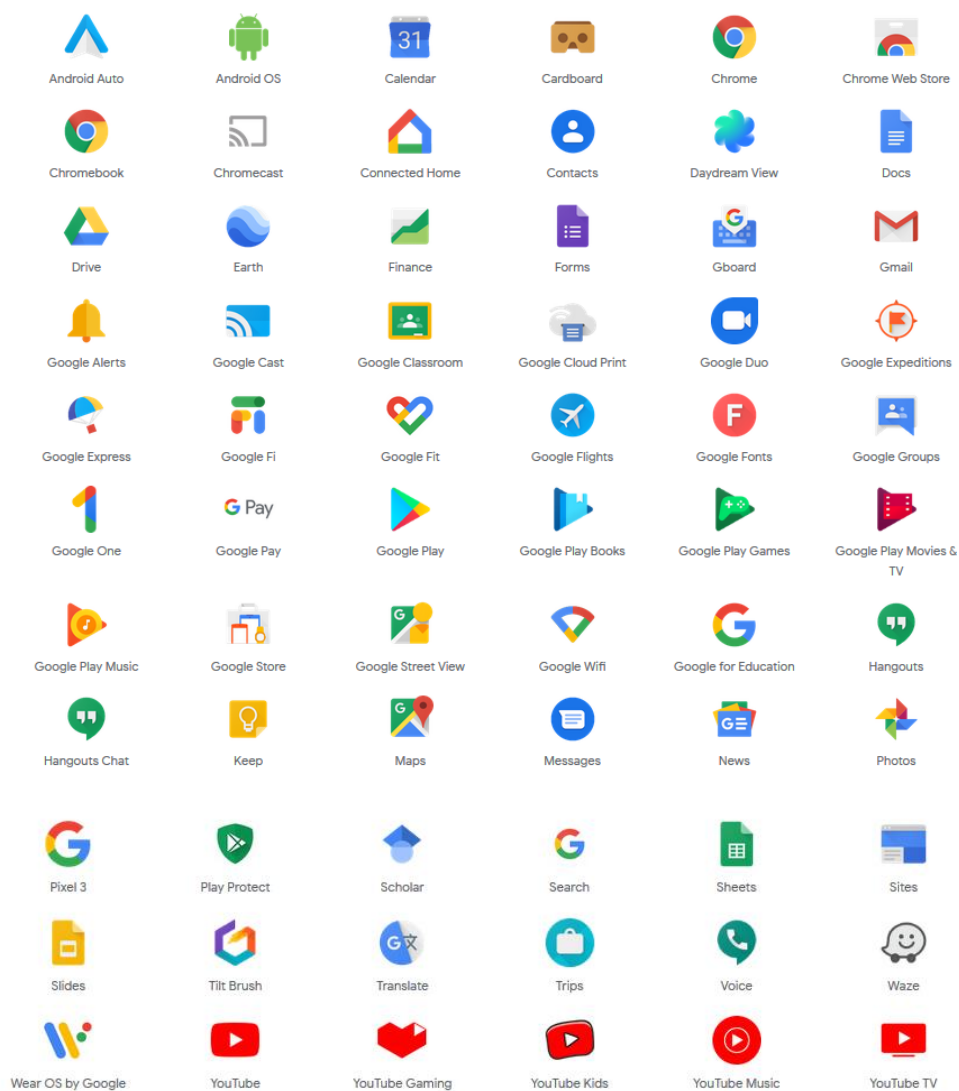


Gráfico 31: Productos de Google "para todos"

### Productos para negocios (Productos de Google):

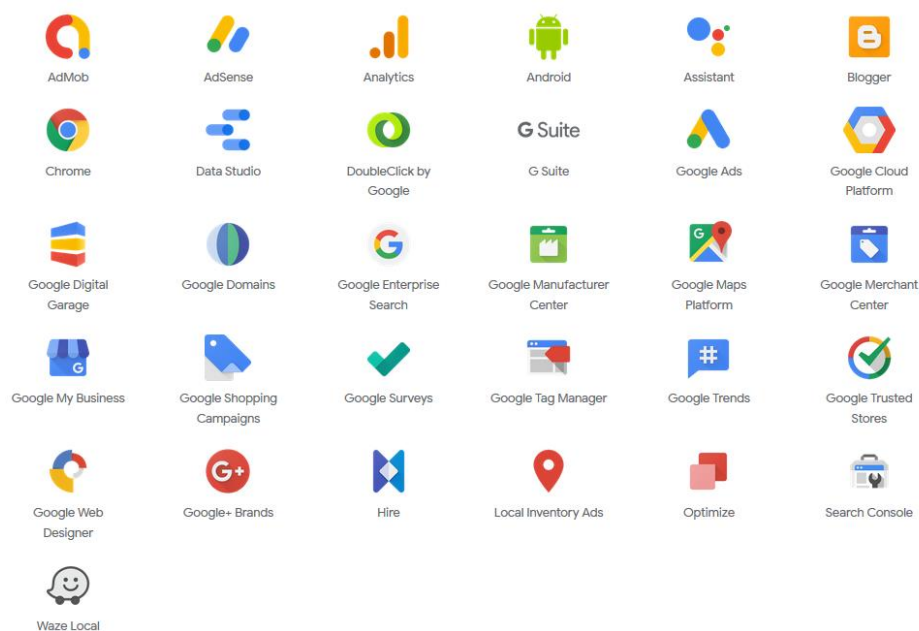


Gráfico 32: Productos de Google "para Negocios".

### Productos para desarrolladores (Productos de Google):

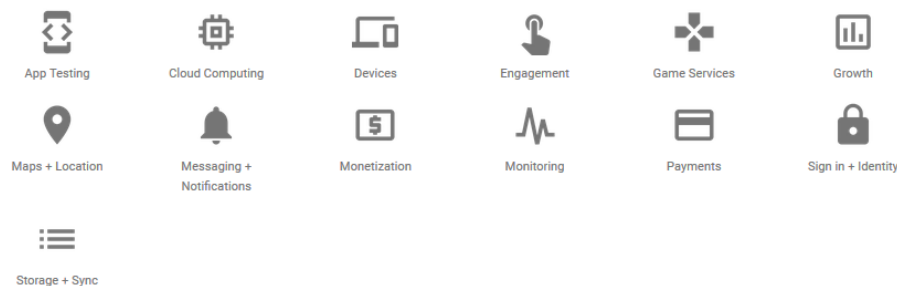


Gráfico 33: Productos de Google "para Desarrolladores".

En muchos casos, para hacer uso de estas herramientas hace falta contar con una cuenta de Google, e iniciar sesión con ella (es decir, ingresar identificación de la cuenta y contraseña). Este inicio de sesión no es más que identificarnos ante Google. Es decir, dar a conocer quiénes somos, para luego facilitar al gigante tecnológico toda la información al usar sus herramientas tal como describe este apartado. Esto también aplica para las actividades realizadas a través de dispositivos móviles con sistema operativo Android (propiedad de Google) los cuales también requieren de una cuenta de inicio de sesión, que se ingresa para firmar nuestra aceptación a ser monitoreados.

En nuestro país, casi el 92% de los dispositivos móviles (teléfonos celulares, tablets especialmente) tienen sistema operativo Android. Esto se desprende del Gráfico 34 obtenido de statcounter (Mobile Operating System Market Share Argentina en Statcounter, 2019).

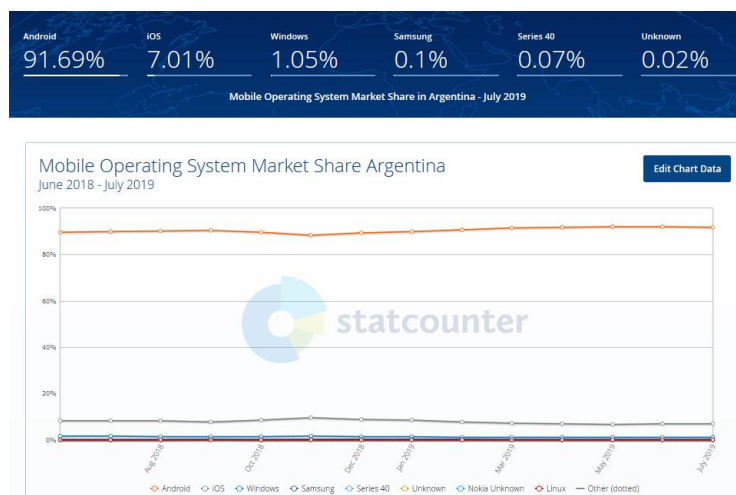


Gráfico 34: Market share de sistemas operativos para dispositivos móviles en Argentina.

Eso significa, que dichos dispositivos tienen configurada una cuenta de Google, a través de la cual, entre otras cosas, se sincroniza la información del correo electrónico, del calendario, se chequea la disponibilidad de actualizaciones.

El número correspondiente a dispositivos móviles con Android, se decrementa a poco más de 76% a nivel mundial (con un 22% de iOS de Apple) lo cual habla a las claras de un todavía muy alto nivel de penetración de Android a nivel global de acuerdo al Gráfico 35 (Mobile Operating System Market Share WorldWide en Statcounter, 2019). Esto sería algo así como 2.500 millones de dispositivos con Android, de acuerdo a (Protalinski, 2019).

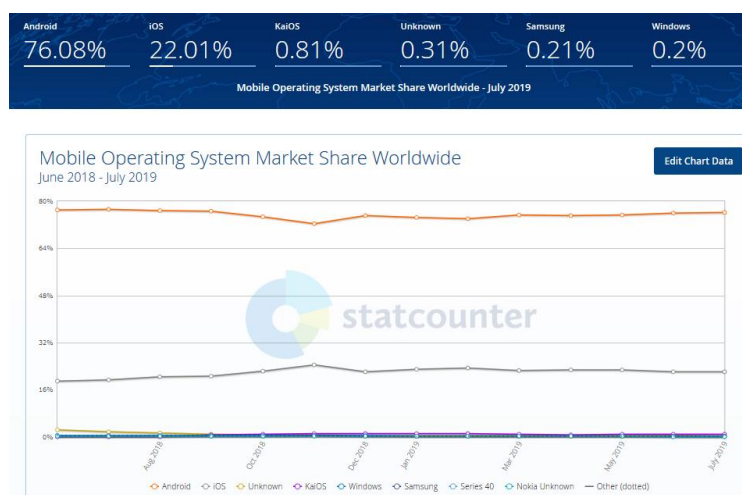


Gráfico 35: Market share de sistemas operativos para dispositivos móviles en el mundo.

En lo que respecta al uso de navegadores (ó browsers), independientemente del tipo de dispositivo (PC, notebook, dispositivo móvil), Google también se encuentra bien posicionado y esto obviamente tiene que ver con las estadísticas que muestran a Android como amplio dominador del mercado de sistema operativo de dispositivos móviles, vistas con anterioridad. Su navegador Chrome, cuenta con el 83,51% del mercado en Argentina (Browser Market Share Argentina en Statcounter, 2019), y con el 63,37% del mercado mundial (Browser Market Share worldwide en Statcounter, 2019) tal como puede visualizarse en el Gráfico 36 y en el Gráfico 37 respectivamente.



Gráfico 36: Market share de navegadores (browsers) en Argentina.

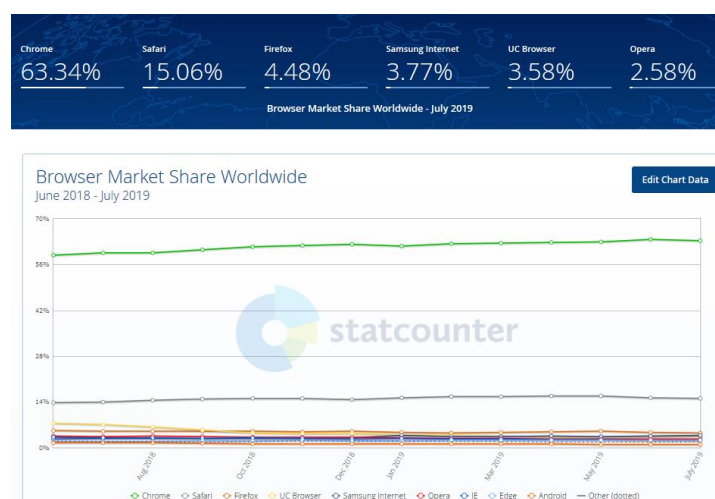


Gráfico 37: Market share de navegadores (browsers) en el mundo.

Esto habla a las claras que con su producto Chrome, Google también es líder en el mercado.

Recordemos que todas las aplicaciones de la suite de Google, son “gratuitas” (o al menos todas sobre las cuales se hará foco en este apartado y que son de interés de análisis). Y como ya se comentara con anterioridad, eso significa que en ese caso, seguramente el producto somos nosotros (o nuestra información). Todos los datos introducidos en las distintas aplicaciones son colectados y cruzados para armar un perfil sobre nosotros.

¿Estamos a esta altura de la lectura en condiciones de plantear la misma pregunta que se realizara al inicio de esta sección? Es decir, ¿Puede el lector ahora tener una idea de la cantidad de datos que ingresa en las aplicaciones de este gigante? ¿Puede imaginar la cantidad de conclusiones que se pueden obtener cruzando toda esa información? Sea cual sea la respuesta, se ha detenido el lector alguna vez a pensar *¿Qué sabe Google de mí?* Si, la respuesta es “muchas cosas”. Pero para tener una idea más precisa al respecto, el lector cuenta con un detalle en el ANEXO III - *¿Qué sabe Google de mí?*

### Hechos que vale la pena conocer

La intención de esta apartado es presentar información, mucha de ella a través de noticias de eventos que se dieron en el mundo, o que están sucediendo en el presente. La finalidad es que el lector tome dimensión de cuánto entra en juego la privacidad, no sólo de los usuarios de internet, sino en muchos casos de toda la ciudadanía.

#### **Monitoreo en China**

China es uno de los países en los que la privacidad no sólo de sus ciudadanos, sino de cualquier persona que pise suelo chino, se encuentra más comprometida a nivel mundial. Prueba de ello son, no sólo las restricciones existentes a la hora de hacer uso de internet, sino además el complejo sistema de monitoreo y vigilancia que ya se encuentra en funcionamiento en varias de las ciudades más populosas del gigante asiático.

Dicho sistema se basa en la instalación de cámaras de video en la vía pública registrando todo el movimiento vehicular y de personas. Las mismas se encuentran conectadas a un sistema dotado de inteligencia artificial que permite el reconocimiento facial en segundos a partir de las imágenes capturadas.

En el año 2018 se estimaba que la cantidad de cámaras instaladas en la vía pública, era de entre 170 y 200 millones, a las que se sumarían otros 450 millones en los próximos dos años.

El cerebro del sistema, es el software denominado Dragonfly Eye (en castellano sería ojo de libélula, y visualizando el Gráfico 38 podemos entender el por qué de dicho nombre), el cual

permitiría identificar al instante una cara entre 2.000 millones de personas con una exactitud del 95,5%.



Gráfico 38: Dragonfly Eye (Ojo de libélula)

“Las cámaras detectan los rostros de todos los usuarios, y los cotejan con la base de datos de personas sobre las que pesan órdenes de búsqueda y captura. En cuanto detecta uno que coincide, envía una alarma a la Policía —que tiene agentes en las estaciones— con los datos del sujeto.”

“Dragonfly Eye ya trabaja con los 1.700 millones de retratos recogidos en la base nacional del gigante asiático, compuesta por las fotografías de sus casi 1.400 millones de habitantes —los nuevos documentos de identidad recogen información específica para ayudar a la identificación por reconocimiento facial— y las de 320 millones de extranjeros retratados en las fronteras —cada vez más equipadas con cámaras especiales— cuando entran al país. Esta información gráfica se complementa con la de las huellas dactilares. La precisión es cercana al 100%”.

“... lee las matrículas, coteja las bases de datos con el modelo y el color del coche identificado, y sirve tanto para determinar si alguien viaja con matrículas falsas como para registrar infracciones de tráfico que descubre” (Aldama, 2018); (BBC - Monitoreo en China, 2017); (Álvarez, 2018)

### **Robo de información a Ashley Madison**

Ashley Madison se trata de una red social especializada en citas extramatrimoniales. En julio del año 2015, un grupo de hackers logró robar información personal de casi 40 millones de usuarios



de dicho portal. Entre los datos robados había nombres completos, dirección postal, información de tarjeta de crédito y sus transacciones, historial de búsquedas entre otra información.

Parte de las razones esgrimidas por los atacantes, fue que el sitio ofrecía a los clientes la posibilidad de eliminar toda la información almacenada, a cambio de unos 20 dólares. Sin embargo, esa información nunca era eliminada de las bases de datos aún luego de realizado el cobro.

“En agosto de 2015, los atacantes publicaron nombres completos, direcciones, números de tarjeta de crédito, correos electrónicos, características físicas, fotografías, preferencias sexuales y hasta conversaciones de unos 39 millones de usuarios del sitio”

“Además, de acuerdo con CNN, unos 15.000 perfiles fueron creados con correos electrónicos del gobierno y militares de Estados Unidos (.gov y .mil), por lo que sus dueños se exponen al cese de sus cargos, la eliminación de su derecho a recibir pensión militar y a penas de hasta un año de cárcel, pues el adulterio constituye una falta grave al Código de Uniforme Militar de ese país.” (Corrales, 2015)

### **Robo de información a Uber**

En el año 2016, atacantes robaron información de más de 57 millones de usuarios de Uber, de los cuales 600.000 eran conductores en EE.UU. La empresa pagó a los hackers 100.000 dólares a modo de “rescate” de la información.

“La compañía rastreó a los piratas informáticos y los obligó a firmar acuerdos de confidencialidad, según las personas familiarizadas con la operación. Para ocultar aún más el daño, los ejecutivos de Uber también hicieron parecer que el pago había sido parte de una “recompensa por errores”, una práctica común entre las compañías de tecnología en la que se le paga a los piratas informáticos para que ataquen su software con el fin de detectar puntos débiles.” (Isaac, Benner, & Frenkel, 2017)

El detalle de todo lo sucedido, saltó a la luz más de un año después.

Para evitar este tipo de prácticas relacionadas a ocultar los incidentes, a partir de la nueva RGPD de la Unión Europea, las compañías están obligadas a reportar los incidentes de seguridad que pudieran sufrir.

A modo de penalidad, por haber ocultado el evento, se le aplicó una multa de 148 millones de dólares. (Ximénez de Sandoval, 2018)

### **Robo de información a Yahoo**

En el año 2013, la conocida empresa Yahoo sufrió el robo de la información asociada a 3000 millones de usuarios. Se trataba de la totalidad de las cuentas que la empresa tenía a la fecha del robo. La empresa dio a conocer la noticia varios años después, e informando que entre la información robada no había contraseñas ni información financiera, pero si nombres, cuentas de correo electrónico, números de teléfono. Entre las personas que poseían cuenta en Yahoo, había funcionarios de alto nivel del gobierno de Estados Unidos.

La información rápidamente se puso a la venta por varios miles de dólares, y de hecho fue adquirida por varios compradores entre los que se destacan enviados de spam, y otros parecerían corresponder a un gobierno extranjero interesado en hackear y u obtener información adicional de funcionarios de otras naciones. (ABC - Yahoo Robo de información, 2017); (NYT - Yahoo Robo de información)

### **Equifax**

Equifax es una entidad financiera de Estados Unidos, la cual en septiembre de 2017 sufrió un ciberataque a través del cual le fue robada la información de más de 140 millones de usuarios. Este ataque es considerado uno de los más importantes no por el volumen de información sustraída, sino por la sensibilidad de la misma.

“En concreto, los hackers se han hecho con el número de la seguridad social que cada cliente tiene asociado a su perfil, su dirección postal y los números de carnets de conducir de clientes de Equifax. Con toda esta información se puede tener acceso al historial de crédito y el perfil financiero de cada una de estas personas.” (Robo de datos Equifax en Infotechnology, 2017)

“La entidad financiera gestiona datos de más de 820 millones de consumidores y más de 91 millones de empresas en todo el mundo. De hecho, los datos robados no provienen únicamente de Estados Unidos. Asimismo, los hackers han accedido a la información de algunos clientes en Canadá y el Reino Unido.”

### **Las elecciones presidenciales de Obama y el Big Data**

Las elecciones para la presidencia de Estados Unidos, llevadas a cabo el día 6 de noviembre de 2012 con la reelección de Barack Obama para ocupar por segunda vez consecutiva el mandato como presidente de dicho país, tuvieron una particularidad que la convirtieron en precedente para las siguientes. La actuación del Big Data. Pero ¿qué es Big Data? Según la definición de IBM (Barranco Fragoso, 2012):

“...utilizado para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a un base de datos relacional para su análisis. De tal manera que, el concepto de Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales.”

El término además, se asocia al análisis de estos enormes volúmenes de datos almacenados, a través del cual se puede deducir o predecir el comportamiento de usuarios a partir de los patrones observados.

En las elecciones del 2012, el equipo de Obama se encargó de combinar grandes volúmenes de información, con modelos predictivos para mejorar sus chances de salir victorioso.

Según el portal Forbes (Méndez, 2015):

“... el equipo de campaña de Obama decidió recopilar toda la información que los ciudadanos estadounidenses publicaban en la red. Así podían saber quién estaba a favor de qué medidas y quién no, mejorando de esta manera sus propuestas y su enfoque.

Además, permitió conocer mejor a los diferentes segmentos en los que sus votantes estaban divididos, especialmente a aquellos sectores más indecisos, y poder convencerlos a través de los medios más adecuados. Por ejemplo, decidieron anunciarse en las pausas publicitarias de la serie Walking Dead o en la revista Reddit, ya que ahí se encontraban los segmentos a los que tenían que convencer.”

“Otro uso que tuvo el big data en estas elecciones históricas fue para lidiar con el complicado estado de Ohio gracias a la geolocalización, conociendo cuáles son las inquietudes de sus habitantes y sabiendo utilizarlas. Y no sólo para saber en qué mejorar, sino también para saber en qué publicidad invertir. Por ejemplo, la cena de George Clooney llevó a las mujeres de entre 40 y 49 años a invertir más en la campaña electoral. Toda una hazaña histórica para una campaña inolvidable.”

De acuerdo a la revista Time (Scherer, 2012):

“... durante los primeros 18 meses, la campaña comenzó de nuevo, creando un sistema masivo que podría combinar la información recopilada de encuestadores, recaudadores de fondos, trabajadores de campo y bases de datos de consumidores, así como de redes sociales y contactos de teléfonos móviles para llegar a los votantes que sabían que podían llegar a modificar su voto. La nueva información recopilada, le dijo a la campaña no sólo cómo encontrar votantes y captar su atención, sino además permitió que los analistas numéricos

realizaran pruebas para predecir qué tipos de personas serían persuadidas por ciertos tipos de apelaciones. Las listas de llamadas en las oficinas de campo, por ejemplo, no sólo listaban nombres y números; también clasificaron los nombres por orden de persuasión, con las prioridades más importantes de la campaña en primer lugar. Alrededor del 75% de los factores determinantes fueron aspectos básicos como edad, sexo, raza, vecindario y registro de votación. Los datos de los consumidores sobre los votantes ayudaron a completar el panorama.

El uso de datos descubrió que las personas que habían cancelado la suscripción a las listas de correo electrónico de la campaña 2008 eran los principales objetivos. Los estrategas elaboraron pruebas para grupos demográficos específicos. Ellos probaron cuánto mejor sería una llamada de un voluntario local que una llamada de un voluntario de otro Estado. Todas las suposiciones realizadas rara vez carecían de números que las respaldaran.”

### **Empresa implanta microchip a sus empleados**

La empresa en cuestión es de origen estadounidense, y se dedica al rubro de la tecnología. Su nombre es Three Square Market. En el año 2017 el presidente de la compañía junto con otros 49 voluntarios, se implantaron un chip subcutáneo del tamaño de un grano de arroz entre los dedos pulgar e índice.

Supuestamente, no molesta ni duele al ser insertado bajo la piel (acción que se realiza a través de una jeringa) ni tampoco al retirarlo (sería una sensación similar a la de retirar una astilla).

A través de este chip, algunas tareas rutinarias tales como acceder a una fotocopiadora (e identificarse como un usuario que puede hacer uso de la misma), abrir una puerta (con la llave bajo la piel), identificarnos en nuestra PC de escritorio, o incluso hasta pagar lo que se consuma en la cafetería de la compañía. El chip tiene información que identifica a la persona que lo contiene, y algo de información médica básica, por lo cual su potencial es enorme. Pero, ¿y la privacidad?

Un año después de su experimento, el chip se insertó en otros 30 empleados más, lo que significa que aproximadamente 80 de los 250 empleados de la empresa ya tenían el chip bajo su piel. (Metz, 2018), (Díaz, 2017)

De otro artículo puede desprenderse de boca del presidente de Three Square Market, que la empresa está trabajando en la evolución del chip de manera tal que a través del mismo se pueda ubicar geo referencialmente a la persona que tiene insertado el mismo (a través de un GPS). A su vez, se pretende incorporar activación por voz, y monitoreo de signos vitales de la persona.

Esto permitiría en un futuro que el chip informe al consultorio médico (o a emergencias) en caso que los signos vitales no sean adecuados, informando además, la ubicación de la persona. (Aiello, 2018)

Esto podría llegar a ser útil para personas que tengan patologías tales como el Alzheimer, en las que la pérdida de la orientación sea un factor frecuente.

Algunas de las descripciones realizadas en este apartado, son al mejor estilo Black Mirror (Brooker, 2011). Para los que no la conocen, se trata de una serie de televisión británica y estadounidense la cual está basada en la incidencia del avance tecnológico sobre nuestras vidas. Se trata de tecnologías inexistentes en la mayoría de sus casos, pero no irrisorias ni imposibles cuando empezamos a conocer ciertas evoluciones tecnológicas que ya existen.

### **Los ciudadanos del mundo bajo vigilancia.**

Ya en este documento, cuando se mencionó a los Gobiernos como uno de los principales enemigos de la privacidad de la información de los ciudadanos a la hora de usar TICs. En el año 2013 gracias a la publicación de documentación ultra secreta de los servicios de inteligencia de Estados Unidos por parte del informático estadounidense Edward Snowden, quedó en evidencia la manipulación de dicha información. Este evento ha tomado tal relevancia en lo que compete al análisis realizado en el presente documento, y ha sido de tal gravedad, que amerita hacer una descripción un poco más detallada del mismo.

Snowden es ex empleado de la CIA (Agencia Central de Inteligencia de Estados Unidos) y de la NSA (Agencia de Seguridad Nacional de Estados Unidos), y por ese motivo tenía acceso a información ultra secreta acerca de la manera en que Estados Unidos junto con otros países aliados, vigilaban las actividades de todos los ciudadanos del mundo. En el año 2013 dicha información fue entregada a medios de comunicación (entre ellos al periódico inglés The Guardian (Ball, The Guardian - Vigilancia Snowden, 2013)).

Snowden brindó detalles sobre el funcionamiento de herramientas informáticas de espionaje del gobierno como XKeyscore y PRISM. Tal como se describe en la publicación del periódico británico The Guardian (Ball, The Guardian - Angry Birds..., 2014) parecen increíbles algunas de las metodologías llevadas a cabo para hacerse de la información de los ciudadanos. Se desarrolló software para aprovechar vulnerabilidades en aplicaciones para teléfonos (apps), tales como el popular juego Angry Birds o Google Maps, y de esta manera tener acceso a la actividad de los usuarios de teléfonos móviles. De esta manera se obtenían datos personales tales como edad, sexo, ubicación, sitios web visitados, listas de amigos, documentos descargados de internet o tamaño de la pantalla del dispositivo, entre otros.

A su vez, y tal como afirma El País (Saiz, 2013) en base a lo publicado por The Washington Post (Gellman & Poitras, 2013) y The Guardian (Greenwald & MacAskill, 2013) a los que Snowden reveló toda la información):

“La Agencia de Seguridad Nacional (NSA) y el FBI han tenido acceso directo y de manera secreta a los servidores de gigantes tecnológicos como Microsoft, Google, Apple o Facebook desde los que han obtenido datos de sus usuarios que les permiten analizar y controlar sus movimientos y contactos”

“El programa secreto en el que supuestamente participaban las agencias de inteligencia y nueve importantes compañías de Internet –Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube y Apple- fue bautizado como PRISM”.

“Los miembros del Congreso que conocían del programa estaban obligados por juramento a no revelar nada sobre su existencia”.

PRISM permitió a la NSA recopilar el contenido de los correos electrónicos, de los archivos enviados o de las conversaciones de chat, audios, videos y fotos.

Respecto a este particular personaje, emblema de la lucha contra el espionaje de los gobiernos, se encuentra disponible un documental multi galardonado (Poitras, 2014), y una película (Stone, 2016) más reciente, en las cuales se explica la manera en la que se desarrolló profesionalmente en las agencias de inteligencia de Estados Unidos, hasta tomar la decisión de publicar la documentación que termina destapando las maniobras de vigilancia.

### **Las TICs y la democracia. El escándalo Cambridge Analytica**

Quizás en nuestro país la situación no haya hecho todo el ruido que merece, pero muy recientemente hubo un gran escándalo mundial en el cual la tecnología ha tenido un rol protagónico. Y fue de hecho la información personal de las personas, y su indebida protección y manipulación la que hizo que todo estallara. Se trata del escándalo desatado por la empresa Cambridge Analytica mediante el uso de información recolectada a través de la red social Facebook.

La compañía británica de análisis Cambridge Analytica, creada en el 2013, impulsó una aplicación (app) a través de Facebook mediante la cual, al descargarla invitaba a los usuarios a contestar una encuesta sobre inclinaciones políticas a cambio de entre 2 y 5 dólares. Dicha app tenía supuestos fines académicos, por lo cual Facebook habría dado el visto bueno, ya que no interfería con sus políticas.

La app fue descargada, y la encuesta respondida en el año 2014 por más de 270.000 usuarios de Facebook, pero se valió de las laxas condiciones de privacidad de esta red social, para hacerse de la información de todos los contactos de esos usuarios.

Las aplicaciones de Facebook piden entre sus requisitos de privacidad, acceso a mucha información. Entre ella y a modo de ejemplo, a la de todos los contactos, el contenido publicado, mensajes, "Me gusta" que se ponen, entre mucha otra. Muchos de los contenidos son compartidos (por ejemplo, fotos en las que se etiqueta a otros usuarios, menciones a otros perfiles o, simplemente, la lista de contactos, cada uno con su respectivo nivel de privacidad).

Esta práctica es común entre las aplicaciones de Facebook. Si bien cada usuario tiene la posibilidad de personalizar esos permisos seleccionando un más alto nivel de restricciones a las aplicaciones (y se recomienda al menos revisarlos), lo cierto es que para la mayoría de las aplicaciones la cesión de altos niveles de permiso y acceso es condición necesaria para la instalación de la misma. Además, los usuarios estaban haciendo uso de una app para supuestos fines académicos, nunca comerciales ni mucho menos políticos. Razón por la cual no tenían de qué preocuparse.

La app permitió recolectar información de 87 millones de usuarios, la cual se utilizó para crear perfiles de votantes y personalizar el contenido de los mensajes (principalmente políticos) que se enviaría a cada uno a través de internet (fundamentalmente mediante el uso de redes sociales) y de esta manera orientar su favoritismo en procesos electorales. Entre otras, hay pruebas que sostienen que este procedimiento habría sido empleado en la campaña presidencial de Donald Trump del año 2016, así como también la del Brexit del Reino Unido (Maza, 2018), (Scott, 2019).

La situación tomó estado público en marzo de 2018 mediante la publicación por parte de The New York Times (Rosenberg, Confessore, & Cadwalladr, 2018) y The Guardian (Cadwalladr & Graham-Harrison, 2018) del testimonio de Christopher Wylie, un informático ex empleado de Cambridge Analytica quien explicó que se logró la maquinaria para manipular las decisiones de los votantes.

Aparentemente, Facebook sabía del hecho desde 2015 y habría solicitado a Cambridge Analytica que eliminara los datos al conocer el uso político que se estaba haciendo de los mismos.

En 2016, se requirieron los servicios de Cambridge Analytica para favorecer las elecciones del candidato republicano Donald Trump, mediante el pago de 6,2 millones de dólares, según datos de la Comisión Electoral Federal. Robert Mercer, estadounidense creador de la compañía, aceptó el encargo, y se lo pudo ver apoyando diferentes iniciativas republicanas. Por su parte,

Steve Bannon, ideólogo de la campaña de Trump y asesor de la Casa Blanca, (hasta agosto de 2017), también pertenecía al plantel directivo de Cambridge Analytica.

Mediante cámaras ocultas, se pudo ver al CEO de Cambridge Analytica reconociendo prácticas para desacreditar políticos a través de internet. Entre ellas, se detalla la campaña realizada en contra de Hillary Clinton, opositora de Donald Trump en las elecciones presidenciales del año 2016 que resultaron con Trump como nuevo presidente de Estados Unidos.

Luego de destaparse el escándalo, Cambridge Analytica anunció su cierre en mayo de 2018 (Ansorena, ABC - Cierre Cambridge Analytica, 2018), (Guimón, 2018).

Luego de este acontecimiento, Zuckerberg (creador y CEO de Facebook) ha debido dar explicaciones ante el Senado (Erice Oronoz, 2018) y en el Congreso (Ansorena, ABC - Zuckerberg Congreso, 2018) de Estados Unidos.

Aseguró que no se trató de una filtración, sino de un uso fraudulento de los datos. Es decir, no hubo una violación al sistema de seguridad de la red social, sino que los usuarios eligieron registrarse en la aplicación, y todos los involucrados entregaron los datos con su consentimiento.

Como consecuencia del escándalo, a fines de julio de 2019 se dio a conocer la multa que deberá pagar Facebook por la filtración de información con Cambridge Analytica. La misma alcanza los 5.000 millones de dólares “como sanción por las malas prácticas en el manejo de la seguridad de los datos de los usuarios.” (BBC - Multa Facebook, 2019), (Pozzi, 2019).

De acuerdo al portal de la BBC, Mark Zuckerberg dijo que la firma tenía “una responsabilidad de proteger la privacidad de las personas”, y que cambiaría la forma en que se desarrollan y funcionan sus productos.

En la plataforma SEDICI de la UNLP se encuentra disponible un documento que explica el caso aquí descripto (Vercelli, 2018).

En julio de 2019 se estrenó un documental titulado “Nada es privado” (Noujaim & Amer, 2019) (su título original en inglés es “The great hack”) que describe de manera minuciosa el detalle del escándalo de referencia, así como también la implicancia que podría tener el mal uso de los datos personales de los usuarios de TICs en la democracia de los países del mundo. En el documental se pone en tela de juicio un gran número de actos electorales en los cuales la empresa Cambridge Analytica habría tenido injerencia empleando la manipulación del electorado a través de mensajes que ayudaran a virar las elecciones a favor de sus “clientes”. Más allá de la veracidad o no de los hechos (hay aquí una enorme cantidad de hipótesis e incógnitas a resolver que obviamente escapan al análisis que se pretende realizar en el presente trabajo de investigación), la intención de exponer este caso particular es la enorme incidencia



que las TICs pueden llegar a tener de manera inconsciente en nuestras vidas. Y sin duda, si se lograra descubrir que son un medio para que algo tan sagrado como los actos electorarios de nuestra querida democracia sea puesta en riesgo, es el momento de como sociedad empezar a hacernos llamados de atención, por lo menos para tener en claro que el riesgo está, que existe. Combatir el fenómeno de las fake news (noticias falsas) es responsabilidad de todos. A modo de cita y sin ahondar en el tema, existe innumerable cantidad de material que explica cómo a través de las noticias falsas, se inician campañas sucias que a la vista está cómo estas pueden afectar una elección, y por ende la democracia que supimos conseguir. (Querido)

La Defensoría del Pueblo de la Ciudad de Buenos Aires a través de un video subido a Facebook, explica cómo detectar las noticias falsas o “fake news”. (Defensoría del Pueblo de la Ciudad de Buenos Aires, 2019)



Gráfico 39: Escándalo Facebook - Cambridge Analytica.<sup>1</sup>

### ¿Qué puedo hacer para protegerme?

Hasta aquí se introdujo al lector en cómo la evolución de la tecnología introdujo nuevos riesgos, y se dieron casos concretos de cómo me podría ver afectado como persona, y hasta como ciudadano. Pero nada se dijo de qué cosas están a mi alcance para protegerme a mí mismo, y a mi preciada información para que no caiga en manos malintencionadas. Lo cierto es que para muchos de los casos vistos hasta aquí, en los que se explicó el robo de información de manera

---

<sup>1</sup> Ilustración: Rodrigo Acevedo Musto, Fuente: <https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica/>

masiva a conocidas plataformas, no hay mucho que se pueda hacer. Al momento de solicitar el alta en las mismas, y aceptar sus condiciones de uso, nuestra información y la privacidad asociada a ella están sujetas no sólo al cumplimiento por parte de las empresas de las condiciones que nos hacen aceptar, sino además, de la manera en que dichas plataformas se protegen (y protegen la información que almacenan) contra los ataques de los hackers.

Las pequeñas cosas que están a nuestro alcance para proteger nuestra información son:

- No tener la misma clave en todas las plataformas.
- Cambiar las claves con regularidad.
- Asegurar el navegador/navegación: El navegador o browser es la principal herramienta empleada para navegar a través de internet y sus sitios web. Debemos asegurarnos que el mismo tenga una versión actualizada para minimizar la explotación de vulnerabilidades del mismo. A su vez, se recomienda el uso de complementos para el bloqueo de programas maliciosos, de tracking o de publicidad que pudieran invadir la privacidad a la hora de usar la red.
- Mantener actualizado todos los productos de software: A medida que pasa el tiempo, a todos los productos de software se le van encontrando “errores de fábrica” muchos de los cuales se convierten en vulnerabilidades que podrían ser explotadas por un atacante, y que podría a su vez realizar algún tipo de daño sobre nuestros activos (ya sea la instalación de software malicioso, o bien robar nuestra información). Quizás nos preguntemos, ¿qué información podría llegar a tener yo que le interese a un atacante para que valga la pena el esfuerzo? La respuesta probablemente sea: Ninguna. Pero debemos tener claro que la gran mayoría de las veces, somos focos de ataques no porque alguien haya querido atacarnos puntualmente a nosotros, sino porque en la enorme red existen innumerables computadoras trabajando de manera autónoma y automática, buscando incansablemente equipos vulnerables sobre los cuales puedan hacer algún daño, o bien, puedan sumar a su ejército de atacantes. Y obviamente, no nos gustaría que nuestro equipo formara parte del ejército de zombis atacantes.
- Instalar productos de software antivirus y firewall. Lo que antes se podría llegar a tomar como opcional, hoy día es obligatorio y aún no suficiente.
- Borrar cookies al salir del browser: Como buena práctica, es recomendable borrar todas las cookies que los sitios por los que vamos navegando crean en nuestra computadora. Las mismas son para ofrecer al usuario una “mejor experiencia de

navegación”. Pero a su vez, son también empleadas por los sitios para trazar nuestra actividad en la web.

- Configurar los ajustes de seguridad y privacidad de los productos empleados a conciencia, de manera tal minimizar la fuga de información personal.
- Mucha precaución a la hora de abrir archivos adjuntos recibidos, o instalar programas de dudosa procedencia. Los mismos podrían incluir código malicioso con dudosas intenciones.
- En caso de ser posible, evitar la paranoia. Todo lo antes expuesto son cosas que hay que saber, conocer que existen, que suceden, que existe la posibilidad que me roben la información, la identidad online y estar atentos haciendo lo que esté al alcance para evitarlo.

Obviamente las medidas de protección antes listadas, sólo protegen nuestra privacidad hasta cierto punto. No hay medidas absolutas que nos protejan de todo. La mejor manera de defenderse, es tener conocimiento acerca de cómo podría ser atacado para obrar en consecuencia. Y ese es en parte el aporte que este trabajo pretende.

## CAPÍTULO IV: Marco legal

Antes de iniciar con el análisis de las regulaciones vigentes en distintos lugares del mundo, vale la pena hacer un paréntesis para referenciar un portal que ha contribuido con mucha información de la que aquí se explaya. Se trata del sitio web de la ONG Privacy International (PI) (Privacy International). Para describir de manera clara qué es y qué hace, podemos decir que es una ONG nacida en Inglaterra, que incluye profesionales de la computación, académicos, abogados, periodistas, juristas y activistas de los derechos humanos, cuyo interés común es el de promover la comprensión de la importancia de la privacidad y la protección de datos a nivel internacional. En la página de esta ONG, hay un apartado en el que se publican informes sobre análisis realizados sobre el estado de la privacidad de distintos países del mundo. Dicho análisis está basado en puntos tales como:

- Marcos legales nacionales e internacionales
- Leyes de vigilancia, agencias, y su supervisión
- Leyes de protección de datos, mecanismos de rendición de cuentas y ejemplos de violaciones
- Sistemas de identidad, incluyendo tarjetas de identificación y registro de votantes

- Ejemplos de sistemas de uso intensivo de datos en una variedad de áreas sectoriales y temáticas.

Los informes se basan en una serie de puntos preestablecidos, obtenidos a su vez de una serie de cuestionarios.

Vale aclarar que el análisis realizado sobre la actualidad de cada país en relación a la privacidad, no está acotada a lo que es la privacidad en el uso de TICs, sino que contempla todos los factores que pudieran poner en riesgo la privacidad de las personas, además de aquellas del mundo tecnológico<sup>2</sup>.

## Europa

En la Unión Europea (UE), una nueva directiva entró en vigencia el día 24 de mayo de 2016, y es de cumplimiento obligatorio a partir del 25 de mayo de 2018 (Reglamento UE 2016/679) (Ley UE 2016/679 - RGPD, 2016). La misma es conocida como GDPR (General Data Protection Regulation) o RGPD en castellano (Reglamento General de Protección de Datos). Se trata de la primera norma relacionada a la temática, que aplica para todos los países de la UE, ya que hasta el momento cada país tenía sus propias reglamentaciones de manera aislada.

Las modificaciones claves de esta nueva legislación respecto a su antecesora de acuerdo al análisis llevado a cabo por el portal no oficial de la nueva reglamentación (GDPR Key Changes):

- Incrementa el alcance territorial: La misma aplica para las empresas que manipulen información relacionada a ciudadanos de la UE, independientemente del lugar de origen o de bandera de las empresas. Este tema era tratado de manera ambigua por las leyes predecesoras.
- Consentimiento: el procedimiento a través del cual los usuarios brindan su consentimiento de términos y condiciones de uso, ha sido fortificado en favor de los usuarios. Las empresas, ya no podrán usar formularios interminables e inentendibles llenos de términos legales. Por el contrario, el consentimiento deberá realizarse a través de un formulario de fácil lectura y entendible por cualquier ciudadano sin conocimientos avanzados de derecho, es decir, en lenguaje plano y claro.
- Penalidades: Las empresas alcanzadas por la nueva legislación, podrán ser sancionados en caso de incumplimiento, con multas de hasta €20 millones, o de hasta el 4% de su facturación mundial anual (lo que sea mayor). Para empresas de la envergadura de

---

<sup>2</sup> Informes de Privacy International por país <https://privacyinternational.org/type-resource/state-privacy>

Facebook o Google estaríamos hablando de sumas multi millonarias. Por ejemplo, para el caso de Google, y teniendo en cuenta las ganancias informadas para el año 2018 según Gráfico 29, la penalidad ascendería a cerca de 5.450 millones de dólares.

- Derechos:
  - Derecho de acceso: Las empresas que gestionan datos sobre las personas, tienen la obligación de informar qué tipo de uso se les dará a dichos datos, cada vez que se desee hacer un nuevo uso, y obtener así consentimiento individual.
  - Notificación ante eventos de seguridad: En caso que la empresa sufriera un incidente de seguridad que pudiera poner en riesgo la información de los usuarios, estos tienen derecho de ser notificados dentro de las 72hs de ocurrido el incidente. Con esto se evitan ocultamientos de incidentes de gran magnitud por parte de las empresas, tal fue el caso de Yahoo del año 2013 (tal como se explicara en el apartado “Robo de información a Yahoo” dentro de la sección “Hechos que vale la pena conocer” en el CAPÍTULO III de este documento).
  - Derecho al olvido: el usuario tiene derecho a solicitar que sus datos sean eliminados cuando por ejemplo, quita su consentimiento sobre el almacenamiento de los mismos, o los mismos fueran tomados de manera ilícita, o los mismos ya no fueran necesarios para la finalidad con los que fueron recogidos.
  - Portabilidad de datos: Los usuarios tienen derecho de solicitar a las empresas, una copia de la totalidad de la información que estas poseen sobre él. Dicha información deberá a su vez, ser suministrada en un formato portable que permita que dichos datos puedan ser importados en otras plataformas.

A través de esta nueva legislación, los ciudadanos de la UE tendrán nuevas herramientas para proteger la privacidad de sus datos en línea. La misma tiene como pilares que las empresas deben informar a los usuarios qué datos están utilizando, cómo los están tratando, para qué y quién es la persona responsable de los mismos bajo pena de grandes multas en caso de incumplimiento.

## Estados Unidos

El tema normativo en Estados Unidos es complejo, dado que cada estado tiene sus propias regulaciones. Esto termina en niveles de seguridad o exigencias diferentes para las empresas,

dependiendo de dónde operen desde el punto de vista de la protección de datos y la privacidad, que es lo que atañe en el presente documento.

Pero en lo que respecta a normativa general, el tema de la privacidad de la información es muy distinto a la Unión Europea. La Ley de la Privacidad data de 1974 y fue consecuencia del Watergate en un momento en el que la privacidad era un atributo muy importante para el pueblo estadounidense. Sin embargo, acontecimientos tales como el atentado a las Torres Gemelas, permitieron al gobierno subordinar muchos derechos civiles a la seguridad de la Nación y a la lucha contra el terrorismo. Así es como apenas días después del atentado, el 26 de octubre de 2001 se aprobó el USA Patriot Act (Ley Patriótica de USA), pero que no es más que el acrónimo de “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act”, es decir “Ley para unir y fortalecer América (Estados Unidos), proveyendo las herramientas apropiadas para impedir y obstaculizar el terrorismo” la cual funcionó como una especie de enmienda constitucional. La misma permitía la vigilancia de la totalidad de las comunicaciones (internet, telefónicas, y hasta la correspondencia).

Mediante la misma, se ampliaron las capacidades de control del Estado, dotando de mayores poderes de vigilancia las agencias de seguridad estadounidenses. Asimismo, la ley también promulgó nuevos delitos y endureció las penas por delitos de terrorismo. La Ley Patriótica ha sido duramente criticada por diversos organismos y organizaciones de derechos humanos, debido a la restricción de libertades y garantías constitucionales que ha supuesto para los ciudadanos, tanto estadounidenses como extranjeros.

En el 2015, aprobó la ley denominada Ley de Libertad (Freedom Act), que puso fin a la recopilación de información a gran escala por parte de la Agencia de Seguridad Nacional (NSA) descubierto por Edward Snowden. Pero la ley continuó permitiendo que las agencias de inteligencia obtengan metadatos almacenados por operadores de telecomunicaciones, al realizar solicitudes caso por caso.

En marzo de 2017, la gestión de Donald Trump aprueba otra medida que genera mucho revuelo entre los usuarios, y los organismos protectores de la privacidad de los internautas en favor de los ISPs. Lo que se hizo es revocar una ley promulgada por su antecesor Barack Obama a través de la cual impedía a los Proveedores de internet comercializar sin previo aviso la información recolectada de los clientes.

Empresas como Google y Facebook cuentan con información de los internautas como la descripta, y de hecho también la comercializan con los anunciantes (tema de discusión y debate). Estados Unidos, en lugar de acotar los derechos de los monstruos recolectores, igualó

las condiciones colocando a los ISPs en igualdad de condiciones favoreciendo una “competencia más equilibrada”. El tema se trata con algo más de detalle en el apartado “Proveedores de Servicio de Internet (ISPs)” dentro de la sección “Qué proteger y de quién” en el CAPÍTULO II de este documento.

Un caso que golpeó duro a Estados Unidos, y que dejó al descubierto la manipulación de la información de los internautas en pos de, en este caso beneficios políticos, ha sido sin lugar a dudas el de Cambridge Analytica, empresa que se hizo con información de más de 87 millones usuarios de Facebook para emplearla con fines políticos, evento que tomara conocimiento público en el 2018. (Dada la relevancia del caso, el mismo ha merecido un apartado titulado “Las TICs, y la democracia. El escándalo Cambridge Analytica” en la sección “Hechos que vale la pena conocer” en el CAPÍTULO III del presente documento).

En marzo de 2018, se adopta la Cloud Act (Ley de la Nube) pero que es el acrónimo de “Clarifying Lawful Overseas Use of Data Act”, o sea “Ley para Aclarar el Uso de Datos en el Extranjero” la cual legaliza la incautación de datos almacenados en servidores ubicados tanto dentro, como fuera de los Estados Unidos. Las principales empresas prestatarias de servicio tipo “nube” de Estados Unidos como sus subsidiarias no tienen más remedio que cumplir, al igual que las compañías internacionales que operan en territorio estadounidense.

Tal como lo explica el artículo de El País (Gavetti, 2018), la ley amenaza la privacidad de los ciudadanos y las empresas europeas (yo agregaría a los de todo el mundo). A su vez, afirma que “La nueva ley permite a los Estados Unidos acceder a datos de empresas y usuarios que estén situados en la Unión Europea, vulnerando las garantías del RGPD”.

En el artículo se explica la ley con un ejemplo sucedido en la vida real:

“En 2013, el departamento de Justicia pidió a Microsoft la entrega de los correos electrónicos de una cuenta presuntamente relacionada con el tráfico de drogas en Estados Unidos. La compañía rechazó esta pretensión porque los datos estaban alojados en servidores situados en Irlanda. Por lo tanto, la solicitud debía tramitarse a través de las autoridades irlandesas, que son las que tienen jurisdicción sobre los datos personales en su país. En 2016, un tribunal de apelaciones dio la razón a Microsoft. Sin embargo, tras la aprobación de la Cloud Act, ante un caso similar Microsoft se vería obligada a suministrar esa información”

“... una agencia gubernamental podría solicitar a una compañía tecnológica, como Google o Facebook, el acceso a correos electrónicos o archivos de una empresa europea alojados fuera de Estados Unidos para comprobar, por ejemplo, si tiene relaciones comerciales con Irán o

participa en alguna licitación en la que concurren empresas estadounidenses. Puede sonar paranoico, pero no olvidemos que entre 2008 y 2009 la Agencia de Seguridad Nacional de Estados Unidos pidió a los servicios de inteligencia alemanes 40.000 datos sobre empresas europeas que no tenían nada que ver con el terrorismo, según denunció la comisión parlamentaria organizada en Alemania a raíz de las revelaciones del ex-analista Edward Snowden.”

En general, las leyes estadounidenses, representan un riesgo para los datos y la vida privada de los consumidores.

Luego de la aprobación por parte de la UE del RGPD, varios estados han realizado modificaciones para adoptar medidas de similares características a las implementadas en la nueva regulación europea, con la intención de darle más transparencia y control a los usuarios. El portal Data Protection Report ofrece un reporte de los Estados pertenecientes a Estados Unidos, que durante el 2018 han modificado sus regulaciones correspondientes a protección de datos (Serrato, Cwalina, Rudawski, Coughlin, & Fardelmann, 2018).

Como mención especial, se puede hacer al Estado de California. El cual, luego de la aprobación del RGPD en la UE, aprobó una norma inaudita para Estados Unidos denominada California Consumer Privacy Act (CCPA) a través de la cual se intenta proteger la información de manera similar a RGPD europeo. (<https://www.caprivacy.org/>)

Según CNN en Español sobre la ley de California, (Heather, 2018):

“La ley, que entra en vigor en 2020, ofrece a los consumidores un amplio control sobre sus datos personales. Les otorga el derecho de saber qué información recopilan compañías como Facebook y Google, por qué lo hacen y con quién la comparten. Los consumidores tendrán la opción de prohibir a las compañías tecnológicas que vendan sus datos, y los menores de 16 años podrán optar entre permitir o no recolectar su información.”

## Latinoamérica

Antes de la entrada en vigencia del RGPD en la Unión Europea en el 2018, varios países latinoamericanos ya tenían algunas políticas orientadas a proteger los datos personales. La aprobación de la nueva legislación europea, desencadenó en la necesidad de rever los estándares vigentes en casi todos los países de Latinoamérica. No sólo para cubrir realidades insatisfechas por normativas que no acompañaron la evolución tecnológica, sino además para



poder dar cumplimiento con los nuevos requisitos establecidos por el viejo continente, muchos de ellos necesarios para dar cumplimiento a estándares obligatorios para el comercio.

## **Brasil**

Aunque parezca extraño, Brasil era uno de los países que carecía de reglamentaciones para la regular la protección de los datos. Mantuvo en su lugar varias leyes con disposiciones algo generales sobre la temática de la protección de los ciudadanos, y sus datos personales:

- El *“Código de Protección al Consumidor”* le daba al consumidor ciertos derechos que le permitían acceder y en caso de así requerirlo, corregir sus datos.
- El *“Marco Legal de Internet”* (Ley 12965/14 (Brasil - Ley 12965, 2014)), aprobado en abril de 2014 regulaba aspectos tales como el tratamiento de datos personales. Entre otras cosas, la norma obligaba a las empresas extranjeras a obedecer las leyes de la legislación local, incluso en los casos en los que no estén instaladas en el país. También obligaba a los ISPs a respetar la inviolabilidad de las comunicaciones de los usuarios, prohibiendo además a suministrar a terceros información de los internautas. La sanción de esta norma, era prioritaria para el gobierno brasilero (en ese entonces en manos de Dilma Rousseff) luego del escándalo destapado por Edward Snowden, quien a su vez afirmara que la Agencia Nacional de Seguridad de los Estados Unidos (NSA) habría espiado correos electrónicos de la presidente, como así también habría realizado escuchas telefónicas suyas (ver apartado *“Los ciudadanos del mundo bajo vigilancia”* incluido en la sección *“Hechos que vale la pena conocer”* en el CAPÍTULO III de este documento).
- El *“Código Penal”*, con su reforma realizada mediante la Ley No. 12737/12 (Brasil - Ley 12737/12, 2012), conocida también como *“ley de delitos informáticos”*, cubría también algunos aspectos relacionados con la privacidad de las personas.

Esta dispersión de disposiciones y normativas, llega a su fin a partir de la aprobación por parte del Senado brasilero de la *“Ley General de Protección de Datos de Brasil”* en el mes de julio de 2018 (Ley 13.709/18) (Brasil - Ley 13709/18, 2018) que se convierte en la primera legislación específica sobre el tema en el vecino país. El texto de esta ley, sigue la tendencia de la Unión Europea con el fin de fortalecer la protección de los datos de los usuarios, garantizando una serie de derechos a los titulares de dichos datos, imponiendo a su vez de varias obligaciones para las empresas recolectoras de información.

La ley entraría en vigencia en el año 2020, de manera tal de darle el tiempo suficiente a las empresas de adecuar los procesos necesarios.

La Ley “General de Protección de Datos de Brasil”, y en concordancia con la Ley vigente de la Unión Europea (RGPD):

- Crea una autoridad nacional de protección de datos.
- Aplica tanto al ámbito público, como al privado.
- Incorpora el alcance extraterritorial. Lo cual implica que el alcance es para empresas que obtienen datos personales de ciudadanos brasileros, independientemente de la nacionalidad de la empresa, o la ubicación de sus servidores.
- Obliga a empresas y organismos gubernamentales que traten datos personales a nombrar un oficial de protección de datos.
- Prevé la imposición de severas multas en caso de incumplimiento.

### **Uruguay**

Tal como se describe en el sitio oficial de la República Oriental del Uruguay bajo el título de “*Cambios recientes a legislación sobre Protección de Datos Personales en Uruguay*” (Uruguay - Nueva legislación de datos personales, 2019):

“En enero de 2019 entró en vigencia la nueva Ley de Rendición de Cuentas, que incorpora importantes modificaciones a la legislación nacional sobre Protección de Datos Personales con el fin ofrecer mayores garantías a los uruguayos. Se trata de la Ley de Rendición de Cuentas (Ley 19.670) (Uruguay - Ley 19670, 2018) promulgada en el mes de octubre de 2018, y vigente desde enero de 2019.”

Hasta ese entonces, la protección de datos personales en el vecino país se regulaba a través de la Ley 18.331 (Ley de Protección de Datos Personales (Uruguay - Ley 18331, 2008)).

Los cambios tienen como objetivo alinear la legislación nacional con los nuevos desarrollos en la materia, ofreciendo así mayores garantías a las personas para la protección de sus datos personales:

- Ampliación del ámbito de aplicación de la Ley de Protección de Datos Personales.
- Nuevas obligaciones para responsables y encargados de bases de datos.
- Modificaciones al “principio de responsabilidad”.
- Creación de la figura del “delegado de protección de datos”.

Todo lo anteriormente mencionado, en línea con las nuevas reglamentaciones RGPD de la Unión Europea.

## **Chile**

En el país trasandino, la protección de datos personales se encuentra regida por la Ley Nº 19.628 (Chile - Ley 19628, 1999), Ley pionera en el tratamiento de la temática para Sudamérica.

Su intención fue la de reglamentar sobre el tratamiento de datos personales de los ciudadanos por parte de terceros. La misma establece que en todos los casos, los titulares de los datos, deben ser informados acerca de los fines de dicho tratamiento, siendo a su vez, obligatorio su consentimiento. Pero no se establecen mecanismos para corroborar el cumplimiento de las obligaciones legales.

Al igual que lo ocurrido con Brasil, y a partir de la legislación aprobada por la Unión Europea, Chile se encuentra en tratamiento de un proyecto de ley que se adapte más a la actualidad, y se acerque más a lo dispuesto por la nueva RGPD. Dicho proyecto de ley estipula entre otras cosas:

- Regula la protección y el tratamiento de datos personales.
- Crea un consejo de protección de datos para hacer cumplir la ley e imponer severas multas en caso de incumplimiento.
- Incluye datos biométricos en la definición de datos sensibles.

La evolución del proyecto de ley puede seguirse a través de los boletines 11144-07 (Chile - Boletín proyecto de Ley 11144-07, 2018) y 11092-07 (Chile - Boletín Proyecto de Ley 11092-07, 2018).

Vale destacar que como se mencionara ya, Chile es un país pionero en lo que refiere a legislación sobre temas relacionados a la protección de datos personales. En tal sentido, con fecha el 16 de junio de 2018 y a través de la Ley 21.096 (Chile - Ley 21.096, 2018), Chile llevó a cabo una reforma constitucional a través de la cual consagra el Derecho a la Protección de los Datos Personales.

## **Colombia**

Colombia posee una diversidad de leyes, decretos además de disposiciones que refieren a la temática de protección de datos personales. Las más importantes son la Ley Nº 1.581 (Colombia - Ley 1.581, 2012) del 2012 y la Ley Nº 1.266 del 2008 (Colombia - Ley 1.266, 2018).

Un proyecto de ley del año 2015 tenía como objetivo ampliar el alcance de la Ley 1.581 con el fin de cubrir aspectos relacionados a la recopilación y el procesamiento de datos personales. A pesar de que el proyecto de ley fue retirado por su patrocinador en junio de 2016, luego volvió a presentarse nuevamente como proyecto de Ley en 2017 (Colombia - Proyecto de Ley 089, 2017) estando a la fecha pendiente su debate.

La nueva regulación RGPD, incorpora un gran número de conceptos basados en la innovación de la tecnología, así como también diversas obligaciones y derechos que no se encuentran contemplados en las leyes colombianas vigentes. Es decir, que se reconoce la necesidad de actualizar la legislación. Esto puede desprenderse del documento “Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital” (Newman Pont & Ángel Arango, 2019) elaborado por Dejusticia, que tal como se puede leer de su portal:

“es un centro de estudios jurídicos y sociales localizado en Bogotá, Colombia dedicado al fortalecimiento del Estado de Derecho y a la promoción de los derechos humanos en Colombia y en el Sur Global. Promovemos el cambio social a través de estudios rigurosos y sólidas propuestas de políticas públicas, y adelantamos campañas de incidencia en foros de alto impacto. También llevamos a cabo litigios estratégicos y diseñamos e impartimos programas educativos y de formación.” (Colombia - Portal Dejusticia, 2019).

Algunas de las obligaciones incluidas en el RGPD, que no se encuentran reguladas por el derecho colombiano, son entre otras el derecho al olvido, la elaboración de perfiles y la designación de delegados de protección de datos.

## **México**

La protección de la privacidad en México está consagrada en el artículo 6 de su Constitución. A su vez México cuenta con varias leyes para el tratamiento de la temática:

- “Ley Federal de Protección de Datos Personales en Posesión de los Particulares” (México - Ley LFPDPPP, 2010): Ley que entró en vigencia en el mes de julio de 2010. La misma incluye aspectos tales como la obtención, uso, transferencia y almacenamiento de dichos datos. Las leyes actuales otorgan derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos personales a los titulares de los datos.
- “Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados” (México - Ley LGPDPPSO, 2017): En vigencia desde enero de 2017. Establece las bases, los principios y los procedimientos necesarios para garantizar el derecho de las personas físicas a la protección de este tipo de datos.

México tiene una estrecha relación comercial con países de la Unión Europea. Teniendo en cuenta este contexto, si bien a la fecha aún no se han llevado a cabo modificaciones en la legislación para acompañar las diferencias que persisten entre esta última y la RGPD, se esperan

en el corto plazo reformas importantes a la ley de privacidad actual para alinear la legislación mexicana con el RGPD.

## **Perú**

Perú cuenta desde el año 2011 con una regulación específica para el tratamiento de la protección de datos personales a través de la Ley 29.733 (Perú - Ley 29.733, 2011). A través de la misma, se regulan los derechos de los titulares de los datos, así como también el cumplimiento de obligaciones de las entidades que incurren en tratamiento de dichos datos.

La Ley fue reformada en el mes de septiembre de 2017 en donde se le incorporó una nueva clasificación de infracciones, así como también disposiciones relevantes relacionadas con la transferencia de datos como ser:

- El responsable del tratamiento deberá notificar cualquier transferencia de datos que resulte de una fusión y/o adquisición de una empresa y de registrar las transferencias internacionales de datos en un registro nacional peruano.
- Nuevas excepciones para obtener el consentimiento para el tratamiento de datos personales, principalmente para prevenir el lavado de dinero y el financiamiento del terrorismo.

Tal como se mencionó con anterioridad, y dada la relevancia de mantener un vínculo estrecho con los países de la Unión Europea desde el punto de vista de los mercados y de la industria, los países de América Latina tienen un verdadero desafío en frente. El desafío es reformar las legislaciones existentes en relación a la protección de datos personales, para poder dar cumplimiento con las nuevas reglamentaciones europeas, además de obtener un reconocimiento internacional en la materia. Todo esto se verá potenciado además, por el incipiente acuerdo entre el Mercosur y la Unión Europea.

## **Argentina**

Nuestro país se encuentra en un estadio de madurez avanzado en lo que refiere a legislación en temas de protección de datos personales. El mismo se encuentra regulado en la propia Constitución Nacional, incorporado en la reforma del año 1994 en el tercer párrafo del artículo 43:

“Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión,

rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.” (Argentina - Constitución Nacional, 1994)

Luego, en octubre del año 2000 se sancionó la Ley número 25.326 (Argentina - Ley 25.326, 2000) titulada “Ley de Protección de los datos Personales” a través de la cual se regularon “Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales”. Tal como se describe en la misma.

### **¿De qué nos protege la vigente Ley?**

La Ley 25.326 estipula que nuestros datos personales sólo pueden ser utilizados si previamente hemos dado consentimiento de ello. De hecho, en su artículo 2 estipula los casos excepcionales en los que nuestros datos podrán ser empleados, sin necesidad de nuestro consentimiento:

“No será necesario el consentimiento cuando:

- a) Los datos se obtengan de fuentes de acceso público irrestricto” (Por ejemplo: boletines oficiales, guía telefónica)
- b) “Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;” (Por ejemplo: Policía, AFIP, ANSeS, Agencias de Recaudación)
- c) “Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;” (Por ejemplo: Padrón electoral)
- d) “Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;” (Por ejemplo: Contrato laboral, información en la relación médico/paciente)

### **¿Cuáles son nuestros derechos a la hora de usar internet?**

Son los detallados en la Ley de referencia. Pero el pasar de los años, y el avance tecnológico han hecho que la misma posea muchas falencias que dificultan su ejercicio. Algunas de ellas son:

- La identificación del origen del sitio web/portal/aplicación que hace la manipulación de nuestros datos personales (obtenidos ya sea a través de una entrega consciente nuestra, o por algún otro medio del cual no fuimos conscientes).
- La identificación de un titular o responsable del sitio/portal/aplicación que manipula nuestros datos. Esta no es una información que se encuentre fácilmente accesible o reconocible en muchos casos.
- Las diferentes legislaciones (en caso que existiera alguna) en los distintos países que pudieran estar involucrados en un litigio o demanda. Las legislaciones suelen ser

ambiguas, y en muchos casos no es claro para sitios cuyos servidores se encuentran en un país, la empresa tiene como origen un país distinto, y para complicarla aún más, nosotros que somos los dueños de la información, estamos en Argentina.

- Por otro lado, casi la totalidad de los sitios/portales/aplicaciones que hacen uso de datos personales de sus usuarios, “obligan” con anterioridad la aceptación explícita por parte de los usuarios de las denominadas “Políticas de privacidad”, de las cuales ya se mencionó algo en el presente documento. Estas políticas en muchos casos (sino en su totalidad) citan párrafos de difícil interpretación, en idiomas distintos al nativo del usuario, que establecen jurisdicciones extranjeras para ejercer escasos derechos otorgados por los términos aceptados (esto es uno de los cambios introducidos por la RGPD en la Unión Europea).

Pero Argentina ha avanzado en cuanto a la legislación. A partir del RGPD, y tal como quedara en evidencia en el análisis de los marcos regulatorios de los países de Latinoamérica, no son pocos los cambios que se han desatado a partir de dicha ley. Y por suerte, Argentina no es la excepción. La ley vigente en nuestro país es del año 2000, y su implementación suele ser compleja y ambigua en algunos casos. Además, no hay que olvidar que tiene por finalidad legislar en temas relacionados con la tecnología, en donde los años introducen avances y novedades que dejan obsoleta cualquier marco que no acompañe dicha evolución.

Hoy día, nuestro país cuenta con un proyecto de Ley para reemplazar la ley vigente, por una nueva dotada de todas las bondades de la directiva ya vigente en la Unión Europea de la cual tanto se ha hablado a lo largo de este documento, como así también del análisis de las distintas normativas vigentes en Latinoamérica.

El documento a través del cual se eleva el Proyecto de Ley al Congreso de la Nación (Proyecto de Ley: LEY DE PROTECCIÓN DE DATOS PERSONALES., 2018) , posee un mensaje justamente dirigido al Congreso, a través del cual se explican las novedades introducidas por el nuevo Proyecto de Ley, y la justificación de la necesidad de contar con una nueva Ley. De dicho mensaje, se destaca lo siguiente:

“... la REPÚBLICA ARGENTINA desde el año 2003 es considerada por la UNIÓN EUROPEA como un país con legislación adecuada para la protección de los datos personales (Comisión de las Comunidades Europeas - Decisión de la Comisión C (2003)1731 de fecha 30 de junio de 2003 con arreglo a la Directiva95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina). Sin perjuicio de esto, se advierte que esta situación puede cambiar con la adopción del Reglamento (UE) 2016/679 (RGPD), motivo

por el cual se propone la presente reforma con la finalidad de mantener los estándares internacionales a los que nuestra legislación supo adaptarse, lo cual traerá consigo nuevas posibilidades de innovación e inversión en nuestro país”

Tal como se describe en el documento antes citado, el proyecto de Ley, tuvo en cuenta las reglamentaciones del RGPD, así como también:




- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)
- Convenio sobre la Ciberdelincuencia (Convención de Budapest)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares de los ESTADOS UNIDOS MEXICANOS y su respectiva reglamentación.
- Ley de Protección de Datos Personales N° 29.733 de la REPÚBLICA DEL PERÚ y su respectiva reglamentación.
- Ley Estatutaria 1581 de 2012 de la REPÚBLICA DE COLOMBIA y su respectiva reglamentación.
- Ley de Protección de Información Personal y de Documentos Electrónicos de CANADÁ (Personal Information Protection and Electronic Documents Act - PIPEDA) (Canadá - Ley PIPEDA, 2000).
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares RIPDD, 2017) (Red Iberoamericana de Protección de Datos) y el Informe del Comité Jurídico Interamericano sobre Privacidad y Protección de Datos Personales (Informe Comité Jurídico Interamericano, 2015).

Los detalles más relevantes sobre el Proyecto de Ley de Argentina antes citado, puede obtenerse en el ANEXO IV titulado “Proyecto de Ley de protección de datos personales. Argentina” del presente documento.



Lo hasta aquí analizado, se resume en el siguiente cuadro:

País/Región	Situación Legal
<p><b>Europa</b></p> 	<p>Nueva legislación en vigencia desde mayo de 2018 que incluye a todos los países miembros de la Unión Europea, enfocada en los usuarios, y en la protección de sus datos personales (RGPD).</p>
<p><b>Estados Unidos</b></p> 	<ul style="list-style-type: none"> <li>- Cada Estado cuenta con sus propias regulaciones.</li> <li>- La histórica “lucha contra el terrorismo” ha subordinado los derechos de los ciudadanos.</li> <li>- Varios ejemplos de recolección indiscriminada de información de la ciudadanía (no sólo de Estados Unidos, sino de todo el mundo).</li> <li>- Algunos Estados avanzaron en leyes de características similares a la nueva legislación europea (RGPD).</li> </ul>
<p><b>Brasil</b></p> 	<p>En 2018 se promulga la “Ley General de Protección de Datos de Brasil” la cual entra en vigencia a partir del año 2020, y está basada en la nueva legislación europea (RGPD).</p>
<p><b>Uruguay</b></p> 	<p>En el año 2019, entró en vigencia su nueva legislación sobre Protección de Datos Personales, la cual está en línea con la nueva legislación europea (RGPD).</p>
<p><b>Chile</b></p> 	<ul style="list-style-type: none"> <li>- Pionero de Latinoamérica en el tratamiento de los datos personales de sus ciudadanos.</li> <li>- En la actualidad cuenta con un proyecto de Ley para adaptar su legislación a la nueva legislación Europea (RGPD).</li> </ul>
<p><b>Colombia</b></p> 	<ul style="list-style-type: none"> <li>- Posee una diversidad de leyes, decretos además de disposiciones que refieren a la temática de protección de datos personales (algunas con más de diez años).</li> <li>- Cuenta con un proyecto de Ley del año 2017 para adecuar su legislación, el cual ahora debería incorporar las bondades de la nueva legislación europea (RGPD).</li> </ul>
<p><b>México</b></p>	<ul style="list-style-type: none"> <li>- Cuenta con legislación de la temática en vigencia desde el año 2017.</li> <li>- Se espera a corto plazo introducir modificaciones en la misma para acompañar la nueva legislación Europea (RGPD).</li> </ul>

	
<p><b>Perú</b></p> 	<ul style="list-style-type: none"> <li>- Cuenta con legislación de la temática en vigencia desde el año 2017.</li> <li>- Al igual que el caso de México, se espera a corto plazo introducir modificaciones en la misma para acompañar la nueva legislación europea (RGPD).</li> </ul>
<p><b>Argentina</b></p> 	<ul style="list-style-type: none"> <li>- Aspectos de la protección de datos personales, se encuentran incluidos en nuestra Constitución del año 1994.</li> <li>- Nuestra “Ley de Protección de los datos Personales” vigente es del año 2000, por lo cual no refleja inmensidad de aspectos relacionados con la evolución de la tecnología.</li> <li>- Existe un Proyecto de Ley para ser debatido en el Congreso desde septiembre de 2018, el cual se basa en las legislaciones de varios países, incluyendo el RGPD de la Unión Europea.</li> </ul>

Si bien aún resta mucho por avanzar en cuestiones legales en pos de la protección de los datos de los ciudadanos, la entrada en vigencia del RGPD en la Unión Europea, ha sido un gran disparador en todo el mundo. En parte por el interés de poder seguir siendo aliado comercial del conglomerado de países europeos. Esto puede verse claramente en los países de Latinoamérica analizados, en los que la legislación europea hizo a casi todos los países a tomar cartas en el asunto. Se trata de una tendencia mundial, de la que ni Argentina en particular, ni Latinoamérica deben estar exentas

El caso de Estados Unidos es un caso particular, en el que la autarquía de cada Estado, sumado al trasfondo de la famosa lucha antiterrorista, y a la actual gestión de un presidente que justamente no es de los que se preocupa por los derechos civiles y ciudadanos, se combinan para formar un combo de libertades parciales. Este panorama ya está presentando no pocas confrontaciones legales entre la Unión Europea y Estados Unidos.

Hay mucho por debatir, y generar conciencia en la ciudadanía, es el primer paso que necesitamos dar para darnos cuenta que nuestra legislación atrasa, y que ni la evolución tecnológica, ni los grandes “consumidores de datos personales” de usuarios de TICs, esperan. Todo lo contrario, se nutren de los vacíos legales, de los grises para operar con absoluta impunidad, y hasta en ocasiones, amparados por la ley.

Lo interesante de todo esto, es que la historia se está escribiendo en este momento. La nueva legislación europea entró en vigencia en mayo de 2018, y de a poco se empiezan a suceder las primeras sanciones “millonarias” a empresas por infringirla.

### Censura digital en el mundo

Así como vemos que en general, el mundo está avanzando en el marco legal en pos de las libertades de los usuarios de internet, aún son muchos los países del mundo que, por el contrario, censuran el libre acceso a mucho del contenido disponible en línea. En este párrafo se hace un análisis de varios países que hoy, en el siglo XXI cuentan con políticas de desinformación de los ciudadanos basadas en la censura de internet:

Los argumentos/excusas pueden estar dadas por cualquier tipo de motivo como ser de índole religiosos, políticos, morales o legales. Algunos de los países que cuentan con restricciones para acceder a los contenidos en la web tal como se detalla en artículo publicado en el portal “The Windows Club” (Gupta, 2019) son:

- **Corea del Norte:** Sólo tienen acceso a menos de 30 sitios web disponibles desde el interior del país. No es de extrañar, su censura está clasificada como una de las más extremas del mundo. El gobierno prohibió oficialmente Facebook, YouTube y Twitter en 2016 como una medida para subrayar su preocupación por la difusión de información en línea. La mayor parte del uso de Internet en el país está restringido al personal militar y al gobierno. Un número muy limitado de ciudadanos del país tiene acceso a Internet y puede ver solo la intranet autorizada por el gobierno.
- **Irán:** Varias redes sociales como productos de software que permiten cifrar las conversaciones por Internet fueron bloqueadas. A partir de 2013, casi el 50 por ciento de los 500 sitios web visitados más importantes del mundo fueron bloqueados, incluidos YouTube, Facebook, Twitter. En 2009, Irán se convirtió en el principal carcelero de periodistas del mundo y desde entonces se encuentra entre los peores carceleros de la prensa del mundo.
- **Vietnam:** el gobierno comunista vietnamita bloquea aquellos sitios web que sean críticos con sus políticas. Redes sociales como Facebook fueron bloqueadas en varias oportunidades, por ejemplo en el 2016 durante una visita del entonces presidente Barack Obama al país para evitar la organización de protestas organizadas a través de la plataforma.

- **China:** La censura de Internet y en especial de las redes sociales en China es una de las más fuertes del mundo. Esto se debe a la gran variedad de regulaciones legales y administrativas. Si bien el acceso a Internet es amplio y está presente una activa industria de redes sociales, el país bloquea las direcciones IP, filtra las búsquedas e incluso borra el contenido o redirige las consultas de contenido restringido a información pro-China. Esta barricada a menudo se denota como “El Gran Firewall Chino”. Durante la última década, China ha bloqueado Google, Facebook, Twitter e Instagram, así como miles de otros sitios web en el extranjero, incluyendo The New York Times y Wikipedia en chino.
- **Arabia Saudita:** Varios libros, revistas, periódicos, películas, contenido y televisión publicados en Internet están altamente censurados en Arabia Saudita por incluir contenido que contrarresta las creencias islámicas, como políticas, sociales y religiosas. Todo el tráfico de Internet en Arabia Saudita pasa a través de un dispositivo supervisado y controlado estrictamente por el Ministerio del Interior (es decir, un departamento del gobierno, responsable de mantener la lista de sitios web permitidos/restringidos). El gobierno bloqueó el acceso a Wikipedia y Google Translate, que estaban siendo utilizados para evadir los filtros en los sitios bloqueados al traducirlos. YouTube no está bloqueado, pero el gobierno ha hecho planes para regular a las compañías locales que producen el contenido para esta plataforma. Las plataformas de medios sociales como Twitter y Facebook son ampliamente utilizadas en el país.

Pueden encontrarse varios portales dedicados a investigar y brindar información sobre el nivel de libertad en el acceso a internet que poseen los distintos países del mundo. A través del mapa ilustrado mediante el Gráfico 40, puede verse de manera sencilla y diferenciado por medio de colores, el nivel de libertad de los distintos países de acuerdo a lo informado en el portal Freedom House que se encarga, entre otras cosas, de analizar aspectos en los cuales la libertad se ve amenazada (Freedom on the Net 2018 Map):

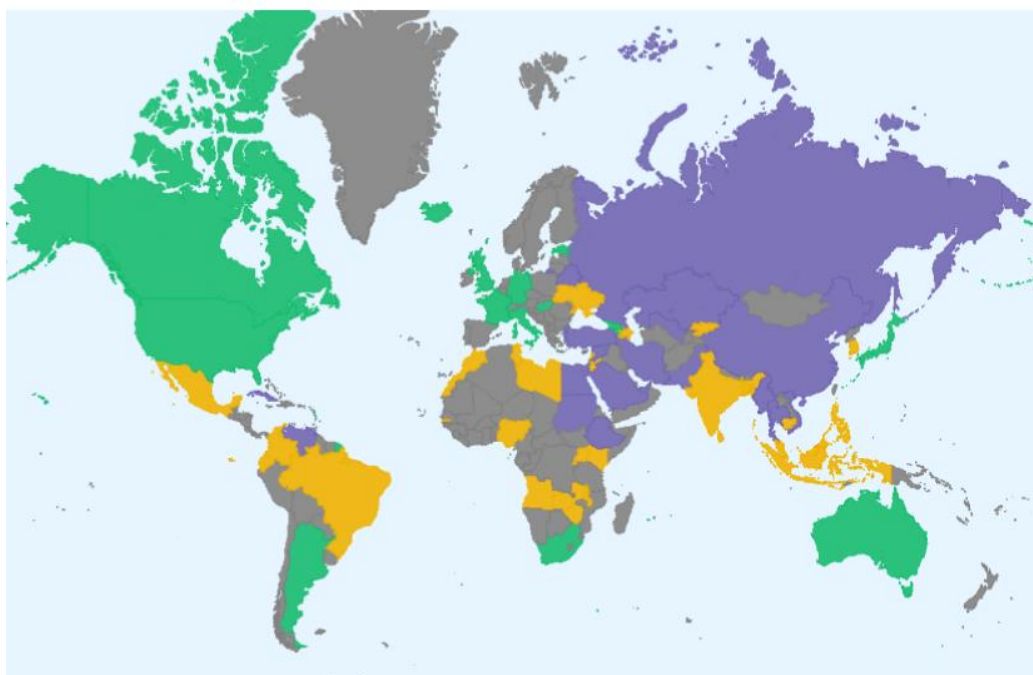


Gráfico 40: Libertad en internet en el mundo. Mapa.

En **verde** los países Libres      En **amarillo/naranja** los parcialmente libres      En **azul/violeta** los países no libres

En el mismo portal también puede observarse de manera más detallada la información de cada país. Para ello se establecen características deseables para la libertad de acceso a internet en los países y se ponderan llegando a un valor referencial para cada país, el cual de alguna manera termina determinando el nivel de libertad de cada uno. El Gráfico 41, tomado del portal de referencia (Freedom on the Net Countries) ilustra los niveles de libertad de diversos países tomados a modo ejemplificador:

Freedom on the Net Countries			
Angola	40/100	Lebanon	47/100
Argentina	28/100	Libya	51/100
Armenia	27/100	Malawi	39/100
Australia	21/100	Malaysia	45/100
Azerbaijan	60/100	Mexico	40/100
Bahrain	71/100	Morocco	45/100
Bangladesh	51/100	Myanmar	64/100
Belarus	64/100	Nigeria	37/100
Brazil	31/100	Pakistan	73/100
Cambodia	55/100	Philippines	31/100
Canada	15/100	Russia	67/100

Gráfico 41: Libertad en internet en el mundo.

También dentro del mismo portal, hay información detallada sobre el estado de situación de Argentina de las libertades en el uso de la red en nuestro país (Freedom on the Net - Argentina).

De ahí, puede destacarse:

“El gobierno no bloquea ni filtra regularmente Internet, y los problemas de eliminación de contenido han mejorado desde que la Corte Suprema de Argentina estableció un sistema de notificación y eliminación judicial en una decisión de 2014.”

“... El gobierno argentino no impone límites al ancho de banda, ni impone control sobre la infraestructura de telecomunicaciones. No se han reportado casos en los que el gobierno haya cortado la conectividad a internet durante protestas o disturbios sociales.”

“Los argentinos continuaron utilizando las redes sociales como una herramienta para la movilización política en 2017. El activismo digital ha jugado un papel crucial en la movilización de protestas para abogar por acciones concretas para reducir la violencia contra las mujeres, desde que el hashtag #NiUnaMenos se volvió viral en las redes sociales en junio de 2015 durante una marcha, continuó estando entre los hashtags más tuiteados durante 2017 y 2018. Cuando en agosto de 2017, Santiago Maldonado, un joven activista de Chubut, desapareció y fue encontrado muerto en octubre, su nombre se convirtió en las palabras más tuiteadas de 2017. Las redes sociales también se convirtieron en una herramienta para la participación política durante las elecciones. Según una encuesta, alrededor del 18% de los usuarios en el área metropolitana de Buenos Aires adquirieron información política de las redes sociales durante 2017, pero este número aumentó al 35% para los menores de 35 años. Los candidatos aumentaron significativamente su campaña en las redes sociales...”

“...En junio de 2016, Argentina se unió a la Coalición intergubernamental Freedom Online, que apoya la libertad de Internet y la protección de los derechos humanos fundamentales. Argentina es el tercer país latinoamericano y el primero de América del Sur en unirse a la coalición.”

“El gobierno argentino no impone restricciones de anonimato o encriptación para los usuarios de internet. Los bloggers y usuarios de Internet no están obligados a registrarse en el gobierno y pueden publicar comentarios anónimos libremente en foros en línea.”

## CAPÍTULO V: El futuro ya llegó

La evolución tecnológica no se detiene. Las novedades surgen todos los días, y estas introducen nuevas amenazas cuyos riesgos de desconocerlas, son muchos. La intención de este capítulo no es realizar un listado exhaustivo de cuáles son esas novedades, sino una vez más, llamar la atención del lector a partir de un par de tópicos emblemáticos que permitan generar interés por la temática, o al menos hacerlo consciente que no se pueden ignorar, dado que desconocerlos podría aumentar la factibilidad de ser víctimas de la tecnología (en lugar de disfrutar sus bondades).

En particular se tratarán dos temas considerados particularmente dentro de esta vorágine evolutiva, dado que, aunque como usuarios no nos interese por conocerlas o por ser parte de ellas, estarán atravesando nuestro día a día de manera irremediable. En conclusión, no hay manera de escaparles.

### Internet de las cosas

La intención de este apartado es introducir al lector en un concepto que pareciera ser novedoso o futurista para aquellas personas que no estén en el diario con las novedades tecnológicas, pero sin embargo ya se encuentra entre nosotros desde hace bastante tiempo. El análisis a realizar no es de tipo científico ni tampoco con un riguroso detalle, sino más bien superficial con el fin de interiorizar en algunos conceptos para luego entender qué riesgo se introducen a partir de este avance tecnológico, y por qué se encuentra incluido en este trabajo de investigación relacionado con la privacidad.

El concepto de IoT (por sus siglas en inglés de Internet of Things) o Internet de las Cosas, refiere a agregar la capacidad a casi cualquier objeto que se desee, de conectarse a Internet.

¿Con qué intención podría llegar a querer conectar las “cosas” a internet? La intención es poder controlar, monitorear, recolectar información y solicitar la ejecución de acciones sobre las “cosas” o por parte de ellas desde cualquier dispositivo conectado a la red, como podría ser desde un teléfono celular, una computadora, una tablet o incluso desde otro dispositivo (o “cosa”) conectada a internet mediante la interacción M2M (machine to machine) prescindiendo de la interacción humana. De esta manera podría tener una serie de dispositivos conectados e interactuando entre sí, cada uno con un rol específico para lograr un cometido final y más importante como piezas de un engranaje más grande.

¿Qué “cosas” podría conectar? Desde sensores y dispositivos mecánicos hasta objetos de la vida cotidiana como pueden ser electrodomésticos (heladeras, lavarropas, aires acondicionados, la

cafetera), el calzado, la ropa, el reloj, las lamparitas e infinidad de etcéteras. Las aplicaciones son casi infinitas.

Si se piensa en aplicaciones industriales, IoT es usado ya en muchas plantas de producción donde los dispositivos y sensores conectados a la red permiten analizar datos, generar alarmas o mensajes que son enviados a los distintos usuarios u operadores para que tomen las acciones necesarias o incluso iniciar protocolos de actuación de forma automática, sin interacción humana, para corregir o tratar dichas alarmas.

Algunos ejemplos de uso doméstico:

- Heladera conectada a la red hogareña a través de WiFi que mantiene registro de los alimentos que contiene, con características de los mismos como ser, stock y fecha de vencimiento. Con esta información, y ante cualquier modificación que debiera ser informada (como stock por debajo del umbral mínimo aceptable, o proximidad a la fecha de vencimiento de un alimento) la heladera podría enviar una notificación, por ejemplo, a nuestro teléfono móvil. Incluso podría notificar estadísticas sobre la cantidad de veces que se abrió la puerta en un lapso de tiempo, temperatura media u otros parámetros. Esto no es futuro. Esto existe hoy y se puede comprar. Sólo para ejemplificar, se ilustra a través del Gráfico 42, un modelo disponible en el mercado (obviamente, sin hablar de precios)

(Fuente: página oficial de Samsung Estados Unidos):



Gráfico 42: Heladera con WiFi



El modelo de la foto, cuenta con 3 cámaras que permiten visualizar su interior a través de las mismas desde cualquier dispositivo móvil, o también desde la pantalla LED del frente, sin necesidad de abrir la heladera.

- Lavarropa conectado a la red WiFi hogareña. El mismo puede ser accedido y configurado desde cualquier dispositivo móvil para elegir ciclos de lavado, recibir notificaciones y mensajes de mantenimiento predictivo. Ejemplos de este tipo de dispositivos, y a la venta en Argentina hay varios. El Gráfico 43 ilustra modelos de lavarropa disponibles en Argentina, todos con las capacidades antes descriptas (Fuente: página oficial de Drean en Argentina).

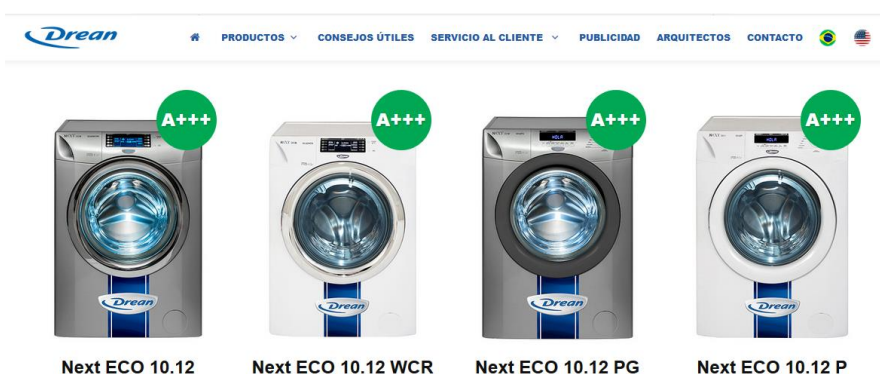


Gráfico 43: Lavarropas con WiFi.

- Otro escenario es el de la domótica. Hoy día ya hay disponibles gran cantidad de dispositivos que se conectan a través de la red WiFi hogareña a internet, para facilitar nuestra vida. Por ejemplo, dispositivos controlados a través de la voz de Google, que tienen incorporado el Asistente de Google, del cual ya algo se dijo en la sección “Google, el oráculo de internet” en el CAPÍTULO III de este documento. A través de los mismos se puede solicitar la reproducción de una lista de canciones (playlist) en nuestro equipo de música o TV, o la reproducción de un contenido desde Netflix. Además, se le puede consultar la cotización del dólar del día, el pronóstico del tiempo, cuánto tardaré en llegar a mi trabajo (en base a la congestión de tráfico), agregar eventos en mi Google Calendar, entre infinidad de tareas más (imaginar las potenciales cosas que se le puede pedir al Asistente de Google). El dispositivo descrito, se comercializa bajo el nombre de Google Home, y se ilustra a través del Gráfico 44 (Google Home).

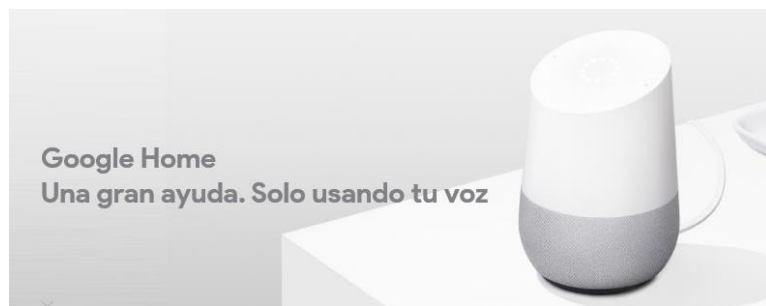


Gráfico 44: Google Home

Otros ejemplos:

- Sistemas de alarmas para casas que se conectan con las centrales, monitoreables desde dispositivos móviles. Los mismos notifican la activación de un sensor.
- Control de la calefacción, o el aire acondicionado de manera remota, para encontrar la casa más confortable a nuestra llegada.
- Relojes pulsera inteligentes (ya vimos un ejemplo en el apartado de este documento que refiere a Google).
- Cámaras de seguridad conectadas a internet para poder ver en vivo y en directo lo que las mismas capturan, ya es algo por demás conocido y empleado de manera cotidiana por un gran número de personas, no sólo en el ámbito industrial, sino en el hogareño para dentro de las casas. Algo similar ocurre con los dispositivos que se emplean para controlar el sueño de los bebés, comúnmente conocidos como baby call. Los mismos ahora contienen capacidad de WiFi para poder ser monitoreados desde cualquier lugar a través de un dispositivo móvil.
- Lamparitas "MagicLight". Controlable desde el teléfono celular (ver Gráfico 45) (Fuente: <https://www.magiclightbulbs.com/>).
  - Poseen temporizadores para programar su encendido o apagado.
  - La luz automáticamente cambia de color para armonizar de acuerdo a la música del ambiente.
  - Más de 16 millones de colores elegibles.



Gráfico 45: Lamparita con WiFi.

- Aires Acondicionados que se conectan a la red WiFi permitiendo su control desde cualquier dispositivo móvil, además de enviar notificaciones por (Fuente: Sitio oficial BGH en Argentina):
  - o Registro de utilización
  - o Necesidad de mantenimiento
  
- Olla de cocción con Wifi: se conecta a la red WiFi hogareña para permitir, desde cualquier dispositivo móvil, ajustar tiempo y temperatura; iniciar o detener la cocción. (Fuente: Mercado Libre)



Gráfico 46: Olla de cocción con WiFi

- Portero eléctrico con cámara: Conecta a la red WiFi hogareña y logra comunicación bidireccional entre el timbre y un dispositivo móvil. Cuando un visitante toca timbre, el sonido se activa y la cámara comenzará a enviar imágenes en tiempo real a través de una llamada al dispositivo móvil (Fuente: Mercado Libre).



Gráfico 47: Portero eléctrico con WiFi

- Sensores de todo tipo (humedad, presión, humedad, temperatura, nivel de agua, nivel de luz, etc) que pueden ser conectados en otros dispositivos para disparar acciones en base a la información obtenida (M2M).

Ejemplos sobran como para entender que esto ya sucede hoy. Que interactuamos todo el tiempo con ello, quizás sin saberlo. Y que con el correr del tiempo la cantidad de dispositivos (ó “cosas”) conectadas a la red irá creciendo hasta alcanzar valores insospechados.

Términos muy relacionados con IoT son "Smart Cities" (ciudades inteligentes) y "Smart Buildings" (edificios inteligentes) en los cuales a través de “cosas” conectadas a la red, se mejora el control del tráfico, el control de los suministros de agua, de luminaria, calefacción en un edificio, el control del transporte público, de semáforos, entre otros muchísimos usos.

### **Algunas Estadísticas**

Según el Portal IOT Analytics (Scully, 2018), la distribución de proyectos de IoT para cada segmento puede visualizarse mediante el Gráfico 48.

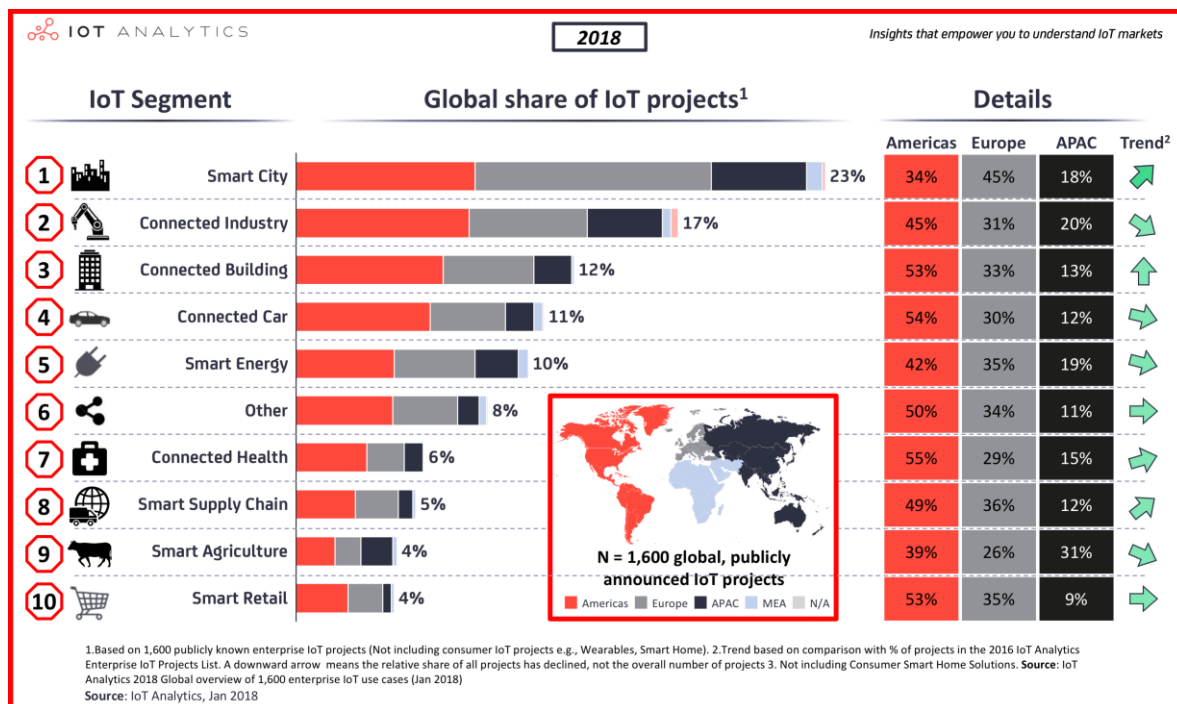


Gráfico 48: Distribución de Proyectos IoT.

Del mismo puede desprenderse que la mayoría de proyectos están relacionados con Smart City (ciudades inteligentes).

A su vez, es interesante ver la cantidad de “cosas” conectadas a la red desde el año 2015, y la proyección de la cantidad que se irán conectando a la red con el correr de los años en todo el mundo hasta el año 2025. Esta información se ilustra a través del Gráfico 49, obtenido del portal Statista (IoT - Crecimiento de dispositivos conectados a la red, 2019):

- Para el año 2019 se prevén 26,66 billones de dispositivos (según la notación estadounidense) conectados a la red, 26.660 millones según la notación empleada en Argentina.
- Para el año 2025 se prevén 75,44 billones de dispositivos (según la notación estadounidense) conectados a la red, 75.440 millones según la notación empleada en Argentina.

Internet of Things - number of connected devices worldwide 2015-2025

**Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)**

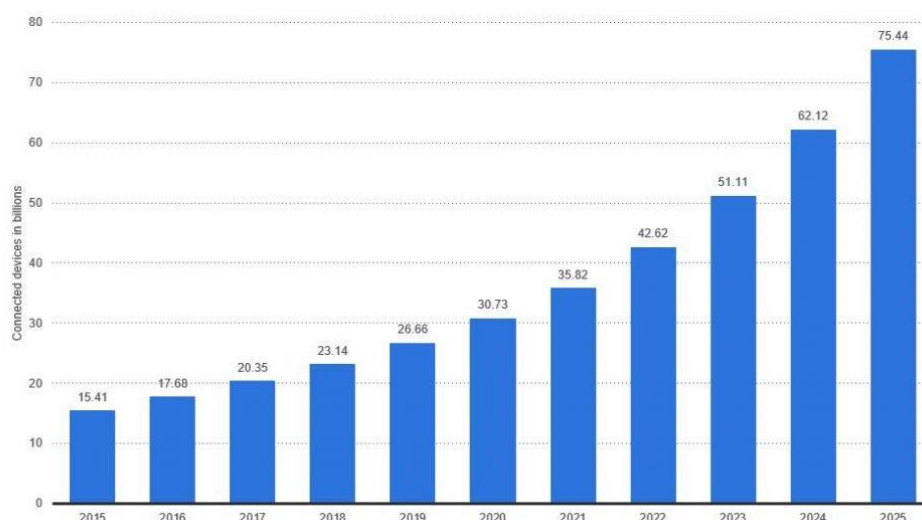


Gráfico 49: Dispositivos conectados IoT en el mundo.

¿Y qué tiene que ver IoT con el tema de la protección de datos y la privacidad, foco de este trabajo? Como se vino tratando hasta aquí, las empresas se han valido casi de cualquier forma para hacerse de la valiosa información de los usuarios conectados a la red. Todo sirve para obtener conclusiones sobre ellos, para luego llevar a cabo distintas acciones. Ya sea, enviar anuncios lo más orientado posible a sus perfiles, robar información para conocer con mayor detalle de una potencial víctima a vulnerar, hasta intentar orientar su elección en una votación (tal como se explicara en el caso Cambridge Analytica tratado bajo el título “Las TICs, y la democracia. El escándalo Cambridge Analytica” en la sección “Hechos que vale la pena conocer” en el CAPÍTULO III de este documento).

A medida que la tecnología nos llevó a estar hiper conectados a través de la mensajería instantánea, de las redes sociales y de tantas otras alternativas que se le ocurra el lector, nuestras vulnerabilidades, o nuestros frentes atacables se han ido incrementado y aún se continúan incrementando. Y el mundo de IoT hace que este incremento casi no tenga límites. Este, como se repitió en varias oportunidades a lo largo de este documento, no es un mensaje en contra de la tecnología, sino una manera de estar atentos y mantener los ojos abiertos. La tecnología ha venido para quedarse, y es una gran herramienta para simplificar nuestra vida cotidiana desde todos los puntos de vista (como ciudadano, en lo laboral, en el entretenimiento y en lo que se nos ocurra). La idea de este apartado no es más que poner en estado de

advertencia a los usuarios que todo lo bueno que introduce la tecnología, y la conexión de las cosas a la red para permitir manejar todo desde dispositivos móviles, para poder medir, monitorear y lograr controles mucho más precisos e incluso, para permitir la interacción de dispositivos M2M prescindiendo de la interacción humana, tiene riesgos. Ese riesgo/costo está relacionado a todo lo que se trató hasta aquí. La información, la exposición para ser atacado. Todo lo que se conecte a la red, será más fácil de ser atacado y vulnerado. Se harán públicas las vulnerabilidades de estos dispositivos conectados a la red, y los ataques y el daño causado a través de los mismos, se empezarán a visibilizar cada vez más.

Las guerras actuales, ya no se libran en los campos de batalla a través de luchas cuerpo a cuerpo entre hombres de carne y hueso tal como era hace varios años o décadas atrás. La ventaja ya no radica en tener un mayor número de hombres desplegados en el campo de batalla. Las guerras hoy se han transformado en guerras de la información. Las potencias mundiales empiezan a librar sus luchas a través de la tecnología, y en el mundo de hoy, el avance tecnológico se ha convertido en crucial para el dominio que varias potencias en el mundo anhelan. Imaginemos el daño que se podría hacer a un país, si se lograra vulnerar de alguna manera la red de una central nuclear, o la red de semáforos, de una ciudad inteligente. Sin duda sería muchísimo, y sin disparar ni un arma de fuego. Por este motivo es que, no son pocos los casos en los que los gobiernos a través de sus agencias de inteligencia, se encuentran involucrados en casos de absorber la mayor cantidad de información, sin importar de qué manera, sin importar la privacidad de las personas, es la guerra de la información.

La evolución tecnológica es algo apasionante, que avanza agregando comodidad y nuevas herramientas al mundo, pero obviamente, no es gratis.

Según la nota en el portal tecnológico xataka (Martí, 2017), y en base a la publicación de información en el portal WikiLeaks (del cual algo se tratara en este documento):

“Las smart TVs y los smartphones habrían servido como micrófonos y cámaras para la CIA....”

“También se habla de ataques a smartphones de modo que éstos envíen información sobre la geolocalización, audios o comunicaciones de texto, pudiendo activar la cámara además del micrófono.”

¿Imaginan poder estar siendo “espiados” por nuestro TV, nuestra cafetera, o nuestro portero eléctrico, dentro de nuestra propia casa? Si estuvieran conectados a internet, serían potenciales focos de ataque. ¿Por qué no? (obviamente la afirmación podría ser algo exagerada, pero la intención es permitir entender que la facilidad de controlar los dispositivos desde un teléfono celular en cualquier lugar de la red, agrega la posibilidad que ese control sea realizado también por alguien malintencionado en caso de ser vulnerada la seguridad).

Las bondades introducidas por las computadoras de abordo que ya casi todos los automóviles incorporan, son muchas y muy buenas, pero ya empiezan a convertirse en un frente de ataque y en un riesgo.

También de acuerdo a documentos expuestos por WikiLeaks, y tal como lo expresa el diario Washington Post (Overly, 2017), la CIA (Agencia Central de Inteligencia de los Estados Unidos) habría investigado la manera de hackear automóviles con la finalidad de llevar a cabo asesinatos casi indetectables.

Siguiendo con el tema de hackeo de automóviles, sobran antecedentes al respecto. Es decir, no hablamos de futurología, sino de cosas que suceden hoy día (y desde hace tiempo). Para citar algunos ejemplos:

Según la nota publicada por Wired (Greenberg, 2016), el fabricante (Chrysler) debió retirar más de 1,4 millones de vehículos marca Jeep del mercado para solucionar el error de seguridad de la computadora que había sido evidenciado por dos expertos en seguridad al vulnerar el sistema desde sus casas conectados a internet. Un año después, volvieron a comprometer el sistema del automóvil (pero ahora desde adentro del vehículo) pero logrando un control casi absoluto del mismo, incluyendo volante, acelerador y freno.

Otra noticia relacionada, es publicada en el portal autopista (del Castillo, 2017) de la cual se cita:

“Expertos en ciberseguridad aseguran que por menos de 40 euros es posible hackear un automóvil que circula a una distancia de hasta 400 metros.”

Según se describe en la página referenciada, con la ayuda de dispositivos de bajo costo, lograron engañar a la computadora de vehículos modernos enviando señales, iguales a las que enviarían los sensores de neumáticos ante la pérdida de presión significativa en algún neumático. El resultado puede ir desde el simple encendido del testigo luminoso en el tablero que indica baja presión en el neumático, a que el vehículo entre en modo de seguridad limitando la velocidad máxima. Algo, sin duda, más que peligroso para la circulación.

A medida que la cantidad de “cosas” conectadas a la red se incrementa, y crezca la cantidad de objetivos atacables por parte de los ciber criminales, empezarán a ser noticias cada vez más comunes las vulneraciones de este tipo de equipos. Quizás hoy en día aún no sean un objetivo lo suficientemente rentable para un atacante. Pero tarde o temprano, todo estará conectado a la red, y los cuidados deberán ser otros distintos.



## 5G

En la actualidad, en muchas zonas de nuestro extenso país, aún no se cuenta con cobertura de telefonía móvil lo suficientemente buena como para establecer una llamada de voz. Ni pensar de contar con cobertura de datos que me permitiera conectar a internet, usar WhatsApp o cualquier otra aplicación a través de 4G (o cualquier de sus predecesores para no ser tan ambicioso).

En base a información publicada por el portal OpenSignal con datos de junio de 2019 (Argentina - Mobile Network Experience Report, 2019), en nuestro país, la cobertura de 4G brindada por cada uno de los mayores tres proveedores de telefonía móvil, se ilustra en el Gráfico 50. De este informe, se desprende además que la cobertura de 4G en nuestro país es de aproximadamente el 79%.

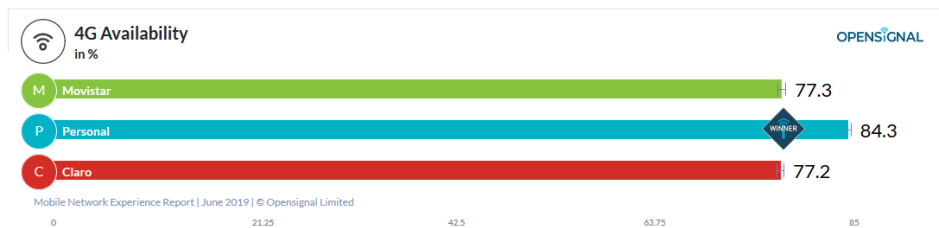


Gráfico 50: Cobertura de 4G en Argentina.

A pesar de esos números, hoy ya se habla de la tecnología sucesora: el 5G. 5G es la quinta generación de las tecnologías y estándares de comunicación inalámbrica, que permiten que nuestros dispositivos móviles se conecten a Internet (no WiFi).

Obviamente esta nueva tecnología presenta características muy superadoras respecto al 4G. En términos de velocidad de transmisión de datos, se prevé que podría alcanzar una velocidad de descarga de entre 1 Gbps (el equivalente a 1000 Megabits por segundo), hasta 10 Gbps (que a priori, parecería algo demasiado ambicioso). Para tener una idea, 1Gbps es la velocidad ofrecida por algunos proveedores de internet en nuestro país para hogares a través de fibra óptica.

En base al mismo reporte de OpenSignal antes citado (Argentina - Mobile Network Experience Report, 2019), los promedios de descarga y subida de los tres mayores proveedores de telefonía móvil en nuestro país, se ilustran en Gráfico 51 y Gráfico 52 respectivamente.

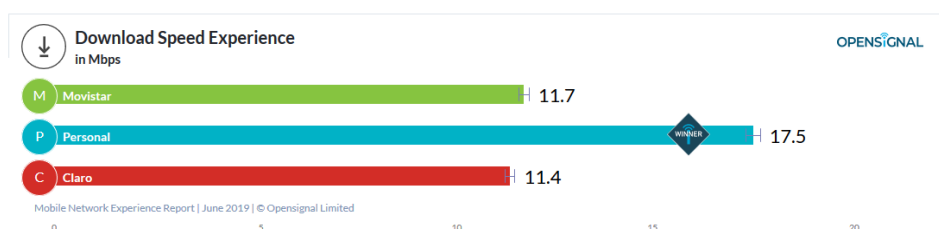


Gráfico 51: Velocidad promedio de descarga en Argentina.

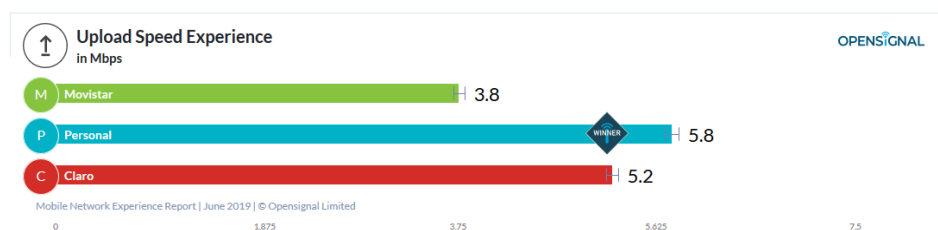


Gráfico 52: Velocidad promedio de subida en Argentina.

En el mes de mayo de 2019, la empresa Personal (Telecom) realizó una prueba concreta con tecnología 5G en un centro comercial situado en CABA, en la cual se alcanzaron picos de velocidad de 1,8 Gbps, y de 700 Mbps en un solo dispositivo mediante pruebas de descarga de contenidos (Mármol, 2019). El pico es más de 100 veces más rápido que el promedio actual de descarga de 17,5 Mbps ilustrado en el Gráfico 51. Obviamente es sólo una prueba, pero sirve para que el lector pueda realizar una comparación y dimensionar las mejoras previstas.

Estas nuevas velocidades permitirían descargar una película en alta resolución en pocos segundos (obviamente contemplando los derechos de autoría correspondientes).

Otra de las características superadoras sobre 4G es que disminuye en teoría, unas diez veces la latencia, que es el tiempo que transcurre, desde que se dispara una orden, hasta que dicha orden se cumple. Pero en la práctica, considerando que la latencia de 5G se presume en 1 milisegundo, y comparando con la latencia actual medida en Buenos Aires e informada por el reporte de OpenSignal (Argentina - Mobile Network Experience Report, 2019) e ilustrada a través del Gráfico 53, la disminución llegaría a 40 veces.

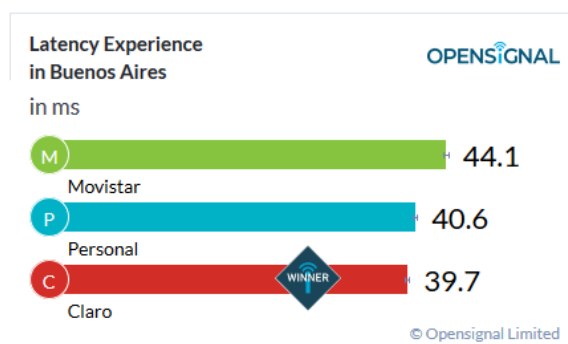


Gráfico 53: Latencia de telefonía móvil en Buenos Aires.

Todo lo hasta aquí expuesto, significa que nuevas tecnologías que requieren de respuestas muy rápidas (como por ejemplo la conducción de vehículos de manera autónoma), dejarían de ser utopías, y podrían ser totalmente realizables. Es decir, 5G presenta características ideales para el desarrollo de IoT, y sin lugar a duda fomentará la explosión de “todo conectado”.

En Argentina, se cree que habrá disponibilidad concreta del 5G recién en 2021 o 2022. Pero estará entre nosotros, y seguramente tendrá una penetración enorme en la población de nuestro país en poco tiempo, tal como sucediera con la transición de 3G a 4G.

Una vez introducido este nuevo concepto, sumado a todo lo que se trató a lo largo de este documento, no caben dudas que el resultado de todo esto será más velocidad y más dispositivos o “cosas” conectadas para multiplicar la información que se genera a través de la red. Sin dudas, es un banquete demasiado tentador para todo aquel que lucra, o se vuelve poderoso a partir de las conclusiones obtenidas en base a la información que recolecta.

A nosotros como usuarios, sólo nos queda estar informados. Seguramente nunca será suficiente para estar exentos a ser víctimas. Pero es a través del conocimiento que se genera conciencia y se dimensionan los riesgos.

## CAPÍTULO VI: Trabajo de investigación de campo.

### La privacidad y los negocios

La manera de tratar la privacidad y la gestión de los datos personales, cala muy profundo en el mundo de los negocios independientemente del tamaño de los mismos. Es decir, que la problemática del tratamiento de los datos, no es sólo de las grandes empresas con millones de usuarios. De hecho, el 43% de los ciber ataques, tienen como objetivo los pequeños negocios (Steinberg, 2019). Esto se debe justamente a que son este tipo de negocios los que en menor proporción están preparados para resistir este tipo de ataques sin que sea comprometida algún tipo de información.

En tal sentido, es de vital relevancia que las empresas (nuevamente, independientemente de su tamaño) sean conscientes del tipo de información que manejan, y de la criticidad que la misma posee, ya sea desde el punto de vista del cliente (cuánto le podría impactar al cliente que la misma sea comprometida) como desde el punto de vista del negocio en sí mismo. Es de gran importancia que las empresas puedan hacer un diagnóstico preciso de cuán importante es la

información que se manipula, y qué impacto podría tener un incidente de seguridad en la continuidad del negocio.

Es por ello, que los negocios deben tomar conciencia y priorizar la forma en cómo se aborda la temática, colocando este ítem entre los lugares de más relevancia de sus agendas.

El impacto y las consecuencias de no hacerlo pueden ser varias, y muy nocivas no sólo desde la perspectiva económica, sino además para las relaciones entre las distintas partes que hacen funcionar el negocio (proveedores, clientes, socios, inversionistas, etc).

A continuación, se detallan algunos de los beneficios (mínimos) que deberían ser tenidos en cuenta por cualquier empresa o negocio, a la hora de decidir qué relevancia y tratamiento le darán a la información que pudieran recolectar cualquiera sea su tipo:

1. Cumplimiento de las normativas.

Sin duda el cumplimiento de la normativa vigente, es el primer ítem a considerar a la hora de citar las bondades de que las empresas inviertan en la privacidad de la información que manipulan. Tal como se mencionara en el CAPÍTULO IV (Marco Legal), la nueva legislación europea prevé altísimas multas a quienes incumplan sus disposiciones. Y esto, no sólo impacta a las empresas europeas, sino a cualquier otra empresa que interactúe con una empresa europea, o bien que almacene información de ciudadanos de la unión europea, por lo cual su espectro de aplicación es verdaderamente amplio. El incumplimiento de esta normativa, cierra las puertas a cualquier empresa a establecer negocios con otras empresas de la UE. Esto significa que el precio de no cumplir las disposiciones, puede llegar a ser demasiado alto. Además de la legislación europea, cabe destacar que nuestro país tiene pendiente el tratamiento de un proyecto de ley, la cual, de aprobarse, dotaría a la Argentina de normativas de muy similares características a las de la UE. Los mismo sucede con otros países vecinos como Brasil, Uruguay, Chile sólo para citar algunos.

Por lo cual, no es menor para una empresa, estar preparada desde el punto de vista normativo, y tener las puertas abiertas para efectuar negocios con empresas de cualquiera de los países antes mencionados.

2. Evitar incidentes que perjudiquen al negocio.

Todas las empresas deben implementar mecanismos que permitan mejorar los aspectos relacionados a la seguridad y la privacidad de la información manipulada. Ninguna está exenta de ello. Los resultados del esfuerzo invertido en dichos mecanismos, junto con los correspondientes controles y sus mejoras, se verán reflejados en la reducción de incidentes de

seguridad que resulten en violaciones de la seguridad y/o privacidad. Y esto a su vez, se traduce en menos infracciones que a su vez podrían resultar en pérdida de la confianza, pérdida de clientes y/o negocios como un efecto dominó. La inexistencia de incidentes, evitará que el negocio tenga que lidiar con multas, sanciones o demandas civiles como consecuencia de las mismas. Y esto, a su vez, permitirá a la empresa poner el foco en el negocio propiamente dicho.

### 3. Evitar incidentes que perjudiquen a los individuos.

Ya se mencionó en párrafos anteriores, la necesidad de implementar medidas que apunten a proveer de privacidad y seguridad a los datos personales. Esto debe suceder en todas las actividades asociadas con la recopilación, el almacenamiento, el procesamiento, el acceso, el intercambio y la eliminación de los datos. De esta manera, minimizando la posibilidad de incidentes de seguridad que pudieran impactar negativamente en el negocio.

Históricamente, las organizaciones no han implementado controles de seguridad de datos completos y sólidos. Es decir, que abarquen la totalidad de la empresa, en cada uno de los puntos en los que podría violarse la privacidad y/o la seguridad de la información, es decir, desde los servidores desde los cuales se disponibiliza la misma, hasta los dispositivos finales de cada uno de los individuos (PCs de escritorio, notebooks, smartphones, tablets, entre otros), sean estos empleados, clientes, socios, proveedores, o visitantes sin compromiso alguno con el negocio en sí mismo.

La implementación de los mecanismos y controles a conciencia para la protección de los datos personales, minimiza la posibilidad de robo de información privada, la cual podría ser usada de manera maliciosa afectando negativamente a los dueños de la misma (es decir, a quien la información refiere). En muchos casos, esa información puede ser empleada para cometer fraudes a terceros. Por ejemplo, empleando información personal robada a una empresa por la implementación de mecanismos débiles en la protección de la misma, una persona malintencionada podría realizar diversos trámites online, compras, adulteración de documentos, a través de una identidad falsa sustentada en la información sustraída, con el natural percance que esto causa al verdadero dueño de dicha identidad. Ejemplos concretos de casos como los aquí mencionados, hay muchísimos. Desde obtención de créditos a nombre de terceros, compras con tarjetas de crédito ya sea de manera online, o de manera física en un local, adulteración de chapas patentes de vehículos automotores, y la lista sigue.

### 4. Los usuarios cada vez exigen más.

Los resultados obtenidos a partir de la encuesta, arrojan que en general, los usuarios no toman muchos de los recaudos recomendables a la hora del uso de TICs. Si bien dichos resultados no permiten concluirlo de manera certera (tampoco tenemos información de años anteriores que permita comparar los resultados), la privacidad cotiza en alza. La actitud de los usuarios respecto al uso de sus datos personales por parte de las empresas tecnológicas, está cambiando. La cantidad de información que puede observarse en la materia, ha crecido muchísimo en los últimos años a partir de los incidentes de seguridad sufridos por empresas de millones de usuarios, en los que datos de usuarios de todo el mundo fueron “robados” de manera maliciosa, con la complicidad de la negligencia. Ejemplo de ello, son casi cualquiera de los casos citados en la sección “Hechos que vale la pena conocer” en el CAPÍTULO III de este documento.

En la actualidad, es común encontrar casi de manera diaria, notas en los diarios online relacionadas a la temática.

El surgimiento de nuevas legislaciones, con la RGPD europea como punta de lanza, y con un proyecto de ley en nuestro país, hablan de un reclamo pendiente por parte de la sociedad, que pareciera que muy de a poco, estaría siendo tenido en cuenta. La necesidad de acotar la potestad sobre los datos recolectados por las empresas (ya sean enormes multinacionales, dueñas de enormes cantidades de información, como pequeños emprendimientos emergentes), se ha vuelto realidad.

Los usuarios demandan poder hacer uso de las TICs de una manera cada vez más privada.

Por el lado de las empresas, tienen en sus manos, la enorme responsabilidad de satisfacer esa demanda creciente de privacidad y protección no sólo de sus usuarios o clientes, sino de todas las personas con las que se interrelacionan y de todas las demás empresas con las que interactúan. El hecho de no hacerlo, es razón suficiente de ser vulnerables a incidentes que podrían afectar de manera letal su imagen y ganancias.

Cada vez más los usuarios necesitan confiar en las empresas a las que le delegan sus datos. Y esto no significa presentar una interminable e ilegible política de protección de datos, que nunca nadie leerá. Significa mostrar un rol totalmente activo en el cuidado y protección de la información que los usuarios le confieren.

Las empresas que entiendan esto, y accionen en tal sentido, verán crecer sus negocios a medida que los consumidores los prefieren frente a sus competidores que así no lo hagan.

##### 5. La privacidad como oportunidad de negocio.

La protección de la privacidad de la información por parte de las empresas, ya no sólo es una obligación (es un deseo que en el mediano o corto plazo, revista tintes legales), sino que además

es una oportunidad para dar visibilidad y hacer crecer un negocio. No sólo para empresas emergentes o pymes, sino también y aún con mucho mayor grado de responsabilidad, para grandes empresas.

Ya se mencionó a lo largo de este documento en reiteradas oportunidades que la evolución tecnológica no va a detenerse, y los negocios que le teman o que no hagan uso de las bondades de la misma, verán limitadas sus oportunidades. La tecnología debe ser uno de los principales socios a la hora de mejorar y optimizar los procesos involucrados en casi cualquier negocio. Actualmente sin ayuda de la tecnología, aspectos que multiplican las oportunidades, tales como el comercio electrónico son imposibles de pensar.

Cada vez hay más usuarios conectados a la red, y a su vez aumenta la cantidad de dispositivos con los que cada usuario se conecta. Esto genera una enorme demanda de productos y servicios, muchos de los cuales aún todavía no existen. Esto lleva a pensar en innovación con el fin de convertir ideas de negocio en enormes oportunidades lo cual puede suceder, en algunos casos, casi en un abrir y cerrar de ojos. No caben dudas que internet es la mayor vidriera que puede existir para un negocio. Por lo cual, exponer un negocio con falencias multiplicará las posibilidades de que su resultado sea el fracaso.

Otra cosa a tener en cuenta es la explosión de IoT (tema tratado en el CAPÍTULO V bajo el título "Internet de las cosas"). Se trata de uno de esos fenómenos que genera la necesidad de nuevos servicios, nuevos productos y nuevas maneras de convivencia e interacción de los negocios. Fenómeno que ya está entre nosotros, y que sin duda, y casi de manera imprescindible, requiere de la tecnología como socia.

Las empresas deben esforzarse para cumplir con las expectativas de los usuarios. La apertura de negocios con mercados más allá del local, podrían aparecer de la noche a la mañana si ofrecemos un producto y/o servicio innovador, y podrían desaparecer en un abrir y cerrar de ojos si no se ofrece confianza en el tratamiento de la información sensible.

Esto obliga a las empresas a cumplir con las normativas locales relacionadas con la privacidad de la información, y en caso de querer mantener negocios con empresas de otro país, estará obligada, además, a cumplir con las normativas vigentes de ese país (teniendo en cuenta que cada vez son más los países que tienen normativas relacionadas). En caso de surgir una nueva posibilidad de negocio, y no estar preparada por cómo se le da tratamiento a la información sensible, lo más probable es que la misma se diluya.

Y es una realidad de la cual ya se explicara en el CAPÍTULO IV (Marco Legal) que luego del RGPD, muchos países están tomando conciencia al respecto, y están desarrollando legislaciones mucho más proteccionistas para con los usuarios. Los negocios, deberían estar preparados desde el

minuto cero para cumplir con esos requisitos legales, para no desperdiciar oportunidades que podrían lamentar luego.

Una frase tomada de un artículo de la revista Forbes (Díaz, 2017) parecería explicar claramente el cambio de tendencia global que se da con los usuarios en el uso de la tecnología asociado a la protección de sus datos:

“Mientras que las empresas de miles de millones de usuarios como Google y Facebook se han construido sobre la recolección de datos, se proyecta que las próximas empresas de millones de usuarios se van a construir en torno a la protección de datos.”

De hecho, la creciente valoración por parte de los usuarios de los aspectos relacionados a la privacidad de sus datos personales, hará que surjan nuevos modelos de negocio. Sólo para citar uno, se puede mencionar ejemplo del monitoreo de la reputación online de un individuo, marca o empresa. Ya se mencionó algo al respecto en la sección “Qué proteger y de quién” – “Reputación online” dentro del CAPÍTULO II, del presente documento, pero la demanda de este servicio, podría aumentar en gran medida a partir de la necesidad (aparentemente creciente) de los usuarios de contar con un perfil online limpio.

Otro aspecto a tener en cuenta, es que el cumplimiento de las legislaciones vigentes en torno a la protección de la privacidad de los usuarios y/o clientes, empieza a convertirse en una herramienta de marketing de las empresas. Se termina apreciando como valor agregado al negocio que empieza a ser tenido en cuenta cada vez más.

#### 6. La privacidad para la construcción de confianza.

Aspectos tales como la creciente toma de conciencia de los usuarios respecto a la manipulación de los datos personales, como el surgimiento de nuevas normativas tales como la RGPD europea, se han convertido en enorme responsabilidad para las empresas que realizan algún tipo de manipulación de información.

Con el uso de las TICs en casi todo, las empresas tienen nuevos desafíos los cuales pueden ser, o bien enormes oportunidades para el crecimiento y proyección de sus negocios, o bien, obstáculos que podrían convertirse en una verdadera pesadilla dependiendo como los mismos sean abordados.

Sobran ejemplos de cómo eventos relacionados con la seguridad y privacidad de la información de los usuarios, afectan de manera directa no sólo las ganancias de las empresas, sino algo mucho más complejo de recuperar que es la imagen y, sobre todo, la confianza. Para ello, basta



con citar los casos descriptos en la sección “Hechos que vale la pena conocer” del CAPÍTULO III de este documento.

Casi sin excepción, las empresas se apoyan (o deberían hacerlo) en mayor o menor medida de infraestructura tecnológica:

- Redes de comunicación.
- Sistemas informáticos tan complejos o simples como uno imagine.
- Bases de datos conteniendo información con distintos niveles de sensibilidad. Por ejemplo, con información relacionada a los clientes, socios, empleados, accionistas, transacciones financieras (compras, ventas, bienes), etc. Que podrían ir desde bases de datos relacionales de gran tamaño, a pequeñas planillas de cálculo.

A su vez, dado que las empresas se encuentran conectadas entre sí, toda esa información es intercambiada y compartida. Esta conexión entre empresas, y el consecuente intercambio de información se da en casi todos los casos. Un ejemplo de ello es el de cualquier tienda que realice ventas de manera online a través de un portal web. En este caso, tenemos por un lado la empresa que aloja el sitio web (como podría ser cualquier empresa que brinde servicio de hosting de sitios web), con las empresas encargadas de la gestión de cobros (por ejemplo Mercado Pago), las que gestionan la logística de entrega a domicilio (por ejemplo las empresas de correo). El intercambio debe ser realizado por todos los que forman “parte del negocio”, de una manera que proteja de manera adecuada, toda la información involucrada. Todas las partes deben prestar atención en detalles relacionados a la manera y tiempo en que se retiene la información de los usuarios (entendiendo por usuarios a todos los involucrados en el negocio: clientes, socios, proveedores, etc); si se comparte dicha información con terceros, y bajo qué condiciones; el nivel de seguridad aplicado sobre la misma (por ejemplo si se emplean mecanismos de encriptación en su almacenamiento y en tránsito en la red); si se cuentan con mecanismos para hacer que la información almacenada expire y en el mejor de los casos, se elimine de manera automática una vez cumplido un período de validez de la misma.

Es decir que todas las partes están obligadas a asumir la responsabilidad, ya que bastará con que uno de los eslabones de esa cadena se rompa, o al menos muestre fragilidad, para que el impacto negativo en el negocio, y en la confianza de sus clientes se haga notar.

Imaginemos cuál sería el impacto en el negocio de una empresa como Mercado Pago (hoy líder en el mercado de cobros) si fuera víctima de un incidente de seguridad en el que se viera afectada la información de los clientes (o de los clientes de sus clientes). Sin duda, el impacto económico, en el negocio podría ser devastador. Y lo sería también para todas aquellas empresas que confían en Mercado Pago para el cobro de sus productos/servicios.

La prioridad de una empresa, debe ser no sólo ganar clientes, sino además obtener su confianza (así como también la de los propios empleados, socios, inversores) que es una de las cosas que hará que el cliente le muestre fidelidad. Ganar esa confianza, puede tomar años. Esta confianza es la que fortalece los vínculos, permite el crecimiento, y favorece al éxito y al crecimiento de un negocio. Es esa confianza la que se desmorona de manera sorprendentemente rápida cuando un incidente relacionado a la privacidad afecta a la empresa.

7. Mantener y mejorar el “Valor de marca”.

No son pocas las organizaciones que sufrieron no sólo pérdidas millonarias, sino además enormes daños a su reputación, y al valor de su marca como resultado de incidentes asociados a la violación de la privacidad. Se pueden tomar nuevamente como ejemplo cualquiera de los casos descritos en la sección “Hechos que vale la pena conocer” del CAPÍTULO III de este documento.

Las organizaciones que no sólo aclaran explícitamente que protegen la privacidad de sus consumidores como uno de sus principales objetivos, protegiéndola y apoyando el cumplimiento de ese objetivo con prácticas de privacidad transparentes, sino que además den muestras sobre el cumplimiento de dicho cuidado, lograrán crear vínculos positivos para con la marca, mejorando además el valor de la misma. Los conceptos negativos que un usuario forma sobre una marca, son muy difíciles de desarraigar, aun cuando la marca haya revertido toda anomalía o comportamiento que llevara a padecer de ese concepto.

Luego de los incidentes en los que Facebook se vio involucrado, como el de Cambridge Analytica, ha invertido fortunas en esfuerzo, en rediseñar sus aplicaciones, en marketing con el propósito de revertir la idea instalada en gran parte de la sociedad de que no se compromete con la privacidad de sus usuarios.

8. Apoyar y ser consecuente con la ética.

No son pocas las empresas que establecen códigos de ética empresarial, a través de los cuales, se establece de qué manera se integran las cuestiones normativas, con las cuestiones relacionadas a los valores (honestidad, moral) en la actividad desarrollada dentro de la empresa. En caso de contar con políticas en este sentido, las mismas deberían indicar aspectos sobre un manejo responsable de la información confidencial. Como por ejemplo, indicar que la misma no se usará en actividades comerciales de manera que resulte perjudicial a su dueño, y que se usará sólo para los fines con los que la misma fue recolectada.

Probablemente de manera fáctica se termine incumpliendo lo que dictamina el código de ética, ya que como bien se describió a lo largo de este documento, a través de la información que se recolecta de los usuarios, es mucho el rédito que se puede llegar a obtener.

### Supuestos y resultados esperados

Los eventos que aportan a la investigación, son de ocurrencia constante, cotidiana. La mayor parte de la información disponible es información presentada por periódicos en línea, o portales de investigación en temáticas relacionadas con la tecnología. Hay muchísima información para analizar, pero la misma se encuentra dispersa y requiere de minucioso tratamiento. La protección de datos personales es un tema relevante y candente en la actualidad, donde diferentes países están definiendo su normativa al respecto.

El mundo está tomando conciencia que lo que está en juego es realmente importante, que ya pasaron muchos años en los que se desatendió el problema. Además de ello, salen a la luz sobradas muestras que las corporaciones y los gobiernos realizan acciones que podrían calificarse como obscenas con el fin de recolectar la información de los usuarios con distintas finalidades y que el daño que causan al hacerlo, es realmente enorme e impredecible. Ejemplos de estas manipulaciones se dieron en el apartado “Hechos que vale la pena conocer” dentro del CAPÍTULO III. Y sinceramente, conocer la existencia de las problemáticas, ayuda a tomar conciencia de lo que está sucediendo y hacer algo por el asunto.

Finalmente, y a partir del puntapié dado por la Unión Europea, los marcos normativos de varios países del mundo están cambiando para proteger más a los usuarios frente a la manipulación de la información llevado a cabo por grandes corporaciones y gobiernos. Este cambio, está teniendo un efecto cascada en otros países del mundo que prefieren legislaciones más proteccionistas entre los cuales se encuentra nuestro país. Estos cambios son hoy. Gran parte de la historia referente a la temática en evaluación, se está escribiendo hoy. En tal sentido, gran cantidad de la información analizada podría cambiar en un futuro no muy lejano.

Se plantea como supuesto, el desconocimiento y en algunos casos hasta desinterés por parte de los usuarios de TICs en general, y en particular de aquellos de la ciudad de La Plata en lo que refiere a la privacidad de sus datos personales que son aquellos sobre los cuales se hace foco a través de la encuesta. La necesidad de pertenecer a la comunidad ofrecida por las redes sociales, y de ser parte de la hiper conectividad, hacen que la aceptación de los “términos y condiciones” de adhesión, terminen siendo un mero trámite como el de completar una planilla para la

asociación a un club. En ningún momento las exigencias, cesiones y renunciamentos detallados en dichas políticas, condicionan, ni ponen en peligro la aceptación de las mismas. En general, dichas condiciones no son tenidas en cuenta por el usuario que las acepta, y en muchísimos casos, hasta ni siquiera son leídas por ellos.

A priori, estos supuestos fueron aprovechados por muchas empresas que se valieron de recursos tecnológicos para lucrar con la información recolectada de sus usuarios. Sería interesante poder concluir si esos modelos de negocio basados en el lucro a partir de la recolección masiva de información, son viables tal como hace algunos años atrás.

La encuesta, contiene preguntas cuya intención es concluir, junto con lo desarrollado a lo largo de la investigación, si realmente la seguridad y la privacidad es un tema que se encuentra en la agenda de los usuarios foco de la presente investigación, o si por el contrario no es algo en lo que se preocupen o presten atención.

A su vez, se desea saber qué nuevas consideraciones deben tener en cuenta las empresas que se valgan de las TICs para realizar negocios con respecto a la seguridad y privacidad de la información que manipulan, y cuáles podrían ser las consecuencias de no tomar las decisiones acertadas.

## Metodología de la Investigación

### Características de la investigación

De acuerdo a lo plasmado en “Metodología de la Investigación” (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010), la presente investigación:

- **Tipo de Estudio:** Se trata de un estudio tipo *descriptivo*, dado que se lleva a cabo una observación de la realidad para analizarla y obtener conclusiones de ella.
- **Tipo de Diseño:** Con respecto al tipo de diseño, se trata de un diseño no *experimental* y *transversal*, dado que se realiza una evaluación de un estado de situación en un momento dado (es decir, una foto).
- **Unidad de análisis:** En este apartado se define cuál es el *algo* que se pretende analizar, y cuál el *alguien* que será foco de investigación. En este caso:
  - o El ALGO objeto de análisis es la privacidad.
  - o El ALGUIEN, sobre el cual se pone foco del análisis, son los usuarios de tecnologías de información y las comunicaciones (TICs) de la ciudad de La Plata.

- **Tipo de muestreo:** Para el caso del tipo de muestreo, el mismo es del tipo probabilístico. Es decir, que todos los miembros de la población, tienen la misma probabilidad de ser extraídos y entrar en la muestra.  
Vale aclarar que el muestreo no es representativo y que los resultados obtenidos no deben extrapolarse por fuera del universo de encuestados. El tamaño muestral no fue calculado en función del tamaño poblacional de la Ciudad de La Plata.

### Recolección de datos

Tal como se mencionó con anterioridad, la recolección de datos se realiza mediante una encuesta (ó cuestionario) compuesta por preguntas de tipo cerradas y disponibles en el ANEXO V de este documento. Esto significa que las alternativas de respuesta han sido previamente definidas para que el encuestado sólo deba elegir entre una o varias de las que mejor describan su respuesta. Al final, se incorpora un espacio de texto libre en el cual se le permite al encuestado introducir su opinión, idea o cualquier otro comentario que desee. Las alternativas de cada pregunta están organizadas de manera tal de permitir la codificación numérica de las mismas.

### Resultados de la investigación

Esta sección contiene el análisis de las respuestas para cada una de las preguntas contenidas en la encuesta.

Si bien las opciones de las preguntas no se encuentran numeradas, para un mejor análisis de las respuestas, en algunos casos se hace mención a alguna opción de respuesta empleando un número. Este número, si bien no se encuentra implícito, refiere al orden de las opciones de respuesta contados de izquierda a derecha, y se emplea de manera de simplificar la apreciación al lector (por ejemplo: *opción 1* u *alternativa 1*, identificando a la primera opción de respuesta de la pregunta).

**PREGUNTA 1: Indicá tu edad**

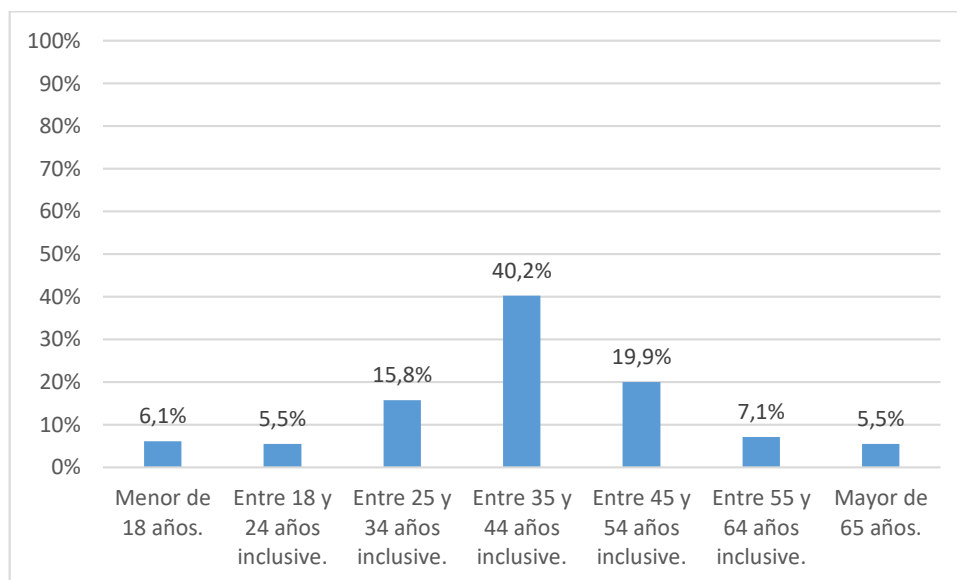


Gráfico 54: Edad de los encuestados.

**PREGUNTA 2: ¿Cuál de las siguientes opciones representa mejor tu género?**

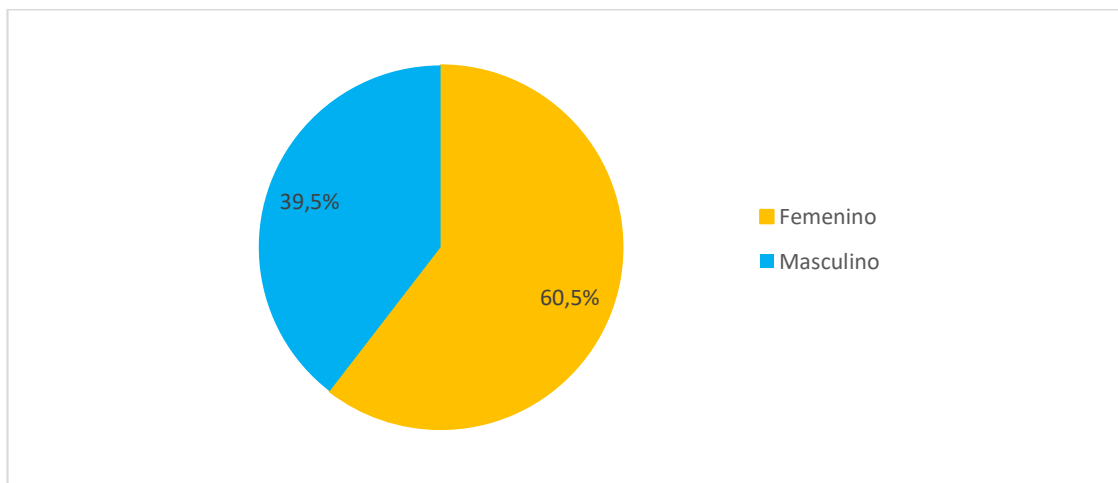


Gráfico 55: Género de los encuestados.

### PREGUNTA 3: Indicá tu último nivel de estudios concluido

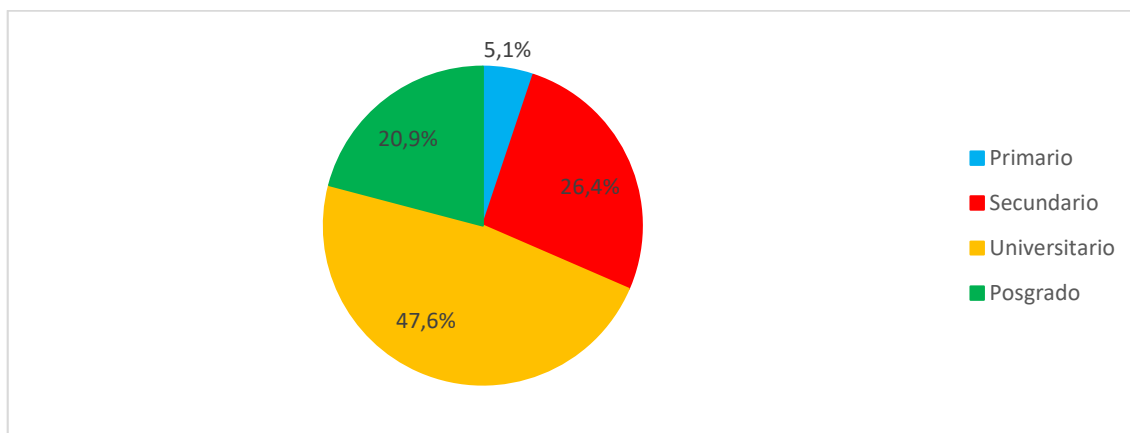


Gráfico 56: Último estudio concluido de los encuestados.

La encuesta tal como fue publicada y contestada, contaba con una opción más correspondiente a la pregunta 3. Dicha opción correspondía a “Ninguno”, que es la opción disponible para aquellos encuestados que no tuvieran ningún estudio concluido. Dado que se recolectaron pocas respuestas con dicha opción seleccionada, se decide quitar las mismas de la evaluación, ya que los análisis obtenidos para aquellos encuestados sin estudios, terminan por carecer de validez debido al escaso universo de encuestados.

El análisis de la pregunta 4 en adelante, se lleva a cabo, por un lado sin hacer ninguna disgregación de los datos. Es decir, sin contemplar ninguna de las tres variables de control antes citadas. Luego se realiza una disgregación de las respuestas, teniendo en cuenta cada una de las tres variables de control. Es decir, se disgregan los datos por edad, por género, y por nivel de estudios.

De todos modos, y con el fin de simplificar el análisis, en el documento quedan plasmados sólo aquellos gráficos de los cuales se permite sacar alguna observación significativa.

**PREGUNTA 4: ¿Qué redes sociales usás?**

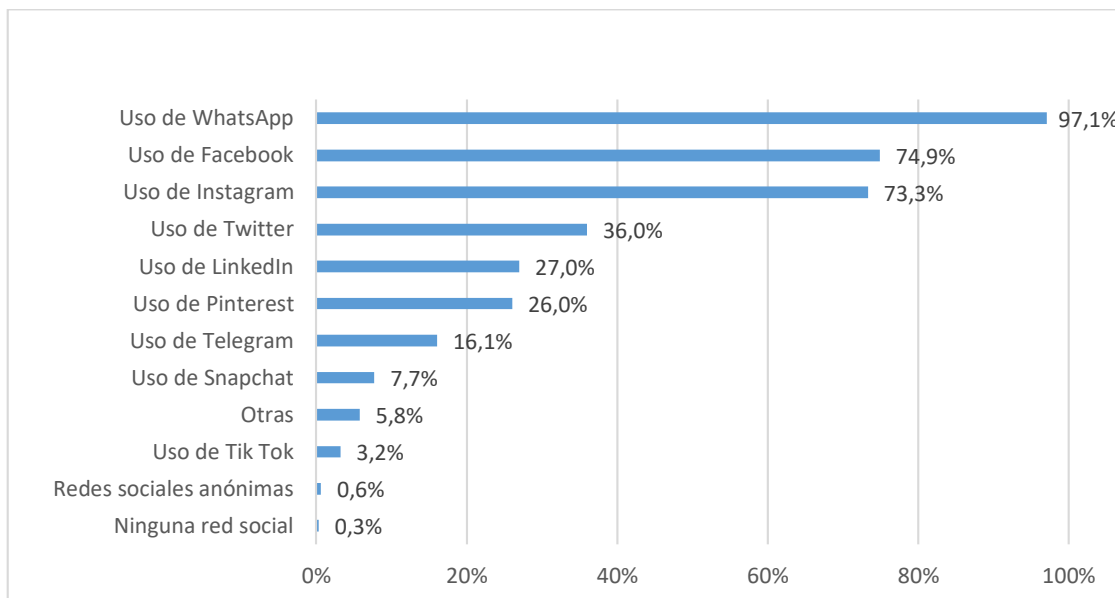


Gráfico 57: Redes sociales usadas por los encuestados.

**Observaciones:**

- Casi la totalidad de los encuestados, usan WhatsApp (97,1%).
- El porcentaje de encuestados que dice usar redes sociales de tipo anónimas es de apenas el 0,6%.

Datos relacionados al uso de redes sociales disgregados por edad:

El análisis se realiza en dos partes. Primero, teniendo en cuenta sólo las tres redes sociales de mayor uso (WhatsApp, Facebook e Instagram), y luego algunas otras redes sociales que vale la pena observar.



Las tres redes de más uso, según Gráfico 57, disgregadas por edad:

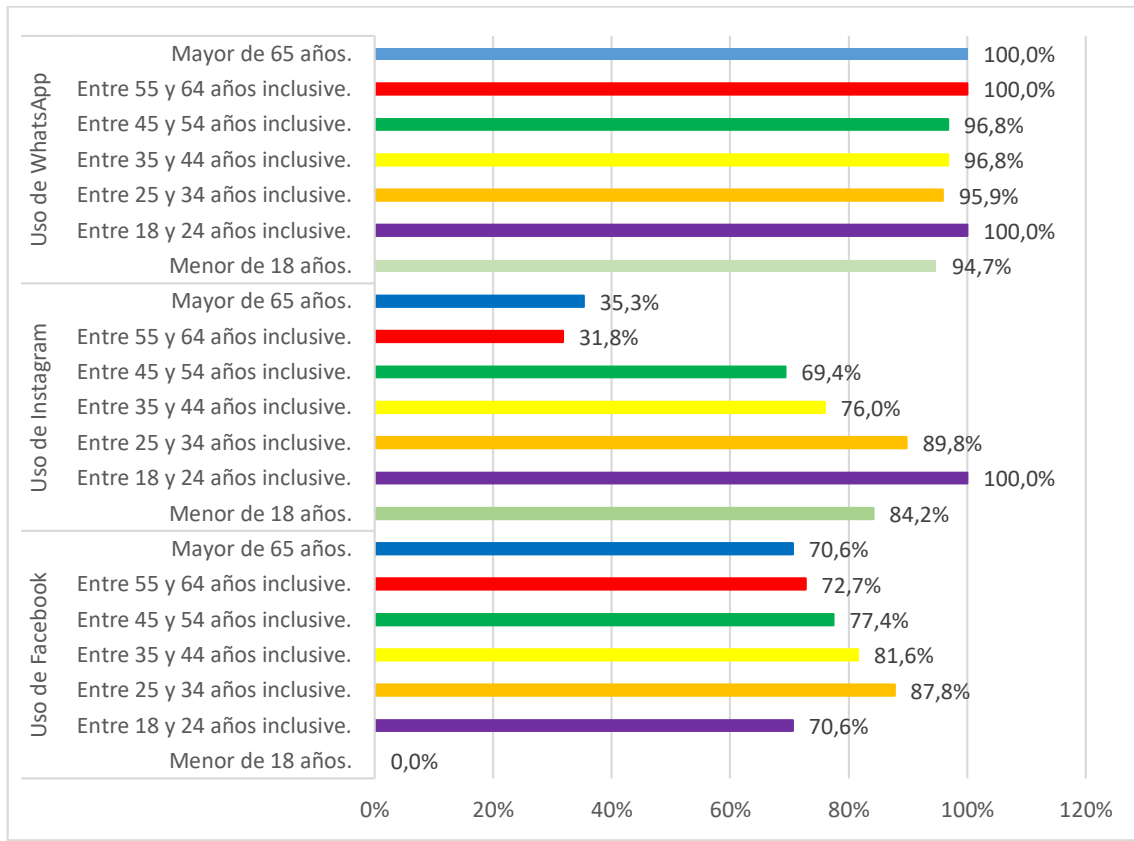


Gráfico 58: Redes sociales usadas por los encuestados, por edad.

**Observaciones:**

- *WhatsApp* es usado por casi el 100% de los encuestados, independientemente de la edad del encuestado.
- Para el caso de *Instagram*, se observa un menor uso en los grupos etarios más grandes. Esto podría deberse principalmente, a que se trata de una red social más “nueva”, que en el último tiempo empieza a desplazar a redes sociales como Facebook. Nótese como el porcentaje de usuarios en esta red social, aumenta a medida que disminuye la edad del encuestado.
- *Facebook* se trata de una red social que ya no sería la más elegida por los nuevos usuarios (menores de 18 años) quienes en su lugar, emplean otras redes sociales (menos empleadas de manera global, pero con una tendencia creciente entre el público de menor edad). En particular, no hay encuestados menores a 18 que hagan uso de esta red social.

Otras redes sociales de menor uso, según Gráfico 57, disgregadas por edad

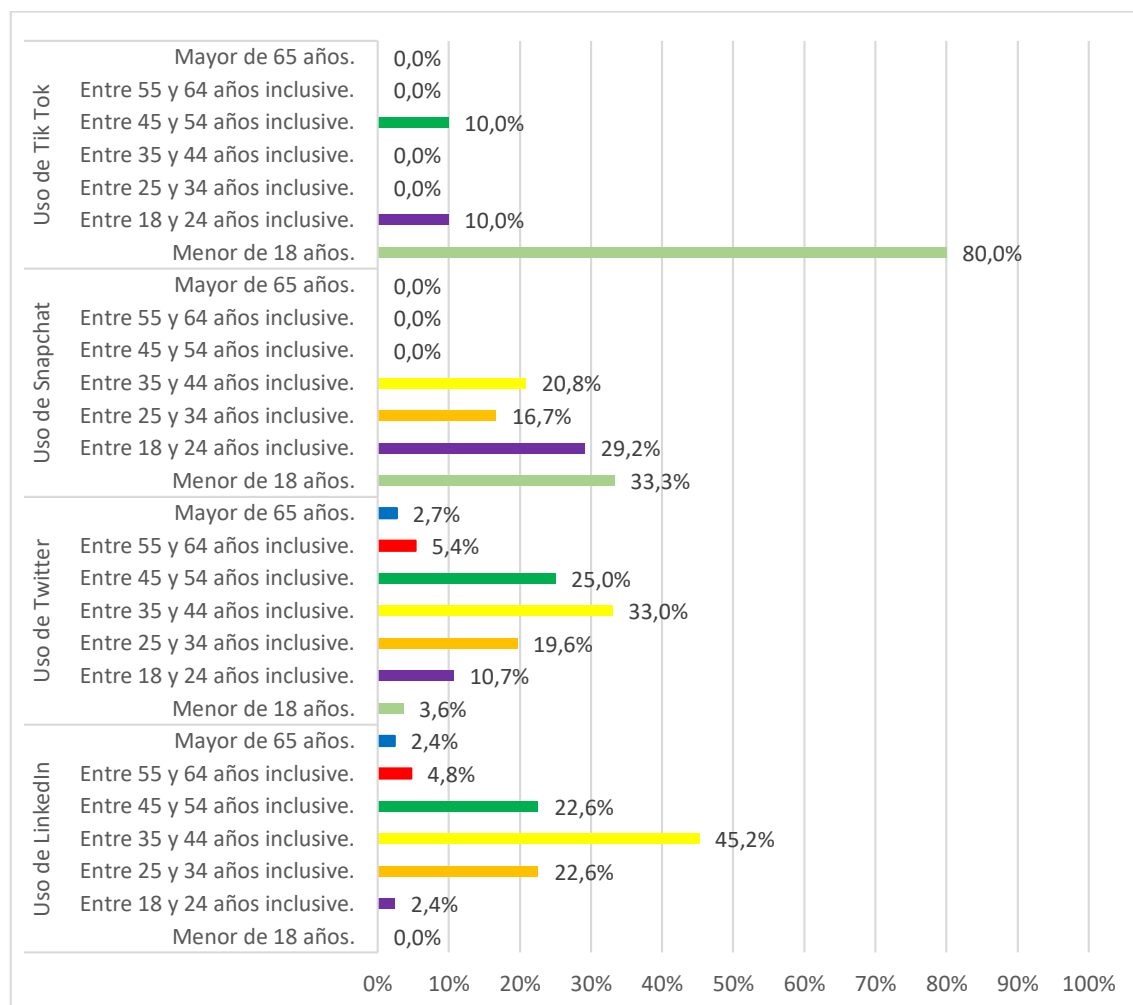


Gráfico 59: Redes sociales usadas por los encuestados, por edad (2da parte).

**Observaciones:**

- *Tik Tok* se trata de una red nueva (año 2017), cuyo uso está en crecimiento en el público más joven.
- De manera similar, pero con mayor distribución entre los grupos etarios de menor edad (y no tan concentrado en los menores), se encuentra *Snapchat*. Se trata de una red social de más años (año 2011), lo cual podría explicar una mayor penetración en un público de hasta el rango etario de entre 35 y 44 años inclusive.
- Para el caso de *Twitter*, se observa una parábola en donde los grupos etarios centrales concentran los mayores porcentajes de usuarios, mientras que los porcentajes decrecen, tanto a medida que aumenta la edad del encuestado, como también a medida que disminuye la misma.
- Algo similar que lo descrito con *Twitter*, sucede con *LinkedIn*. Tal como es de suponer, por la naturaleza de esta red, la misma no es empleada por los menores de 18 años.

**PREGUNTA 5: ¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems?**

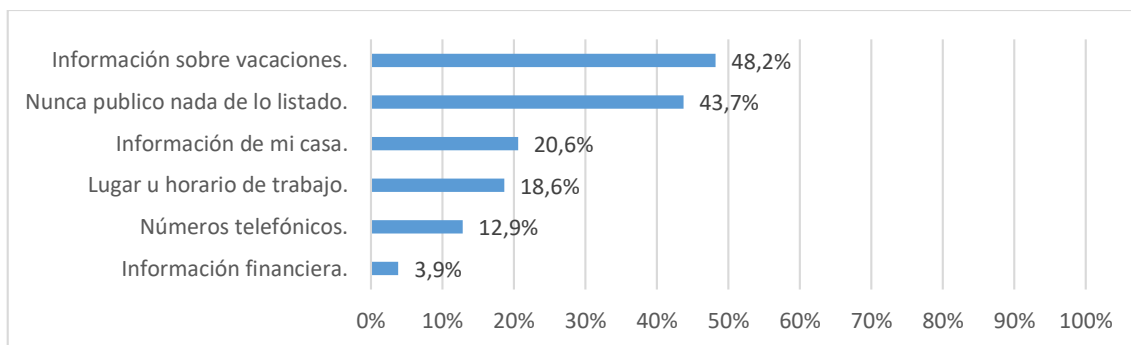


Gráfico 60: Publicación de información sensible (encuesta).

**Observaciones:**

- Del total de encuestados, 43,7% dice no publicar nada de lo listado. Estos encuestados serán analizados con mayor detalle en el presente apartado para determinar si esta respuesta es producto a un alto grado de conciencia en el encuestado que lo lleva a no publicar nada de lo consultado, o bien es simple casualidad o producto de otra razón que excede el resultado observable.
- El 56,3% restante, publica información en base a los porcentajes que aparecen en el gráfico.

Datos relacionados a información publicada disgregados por edad:

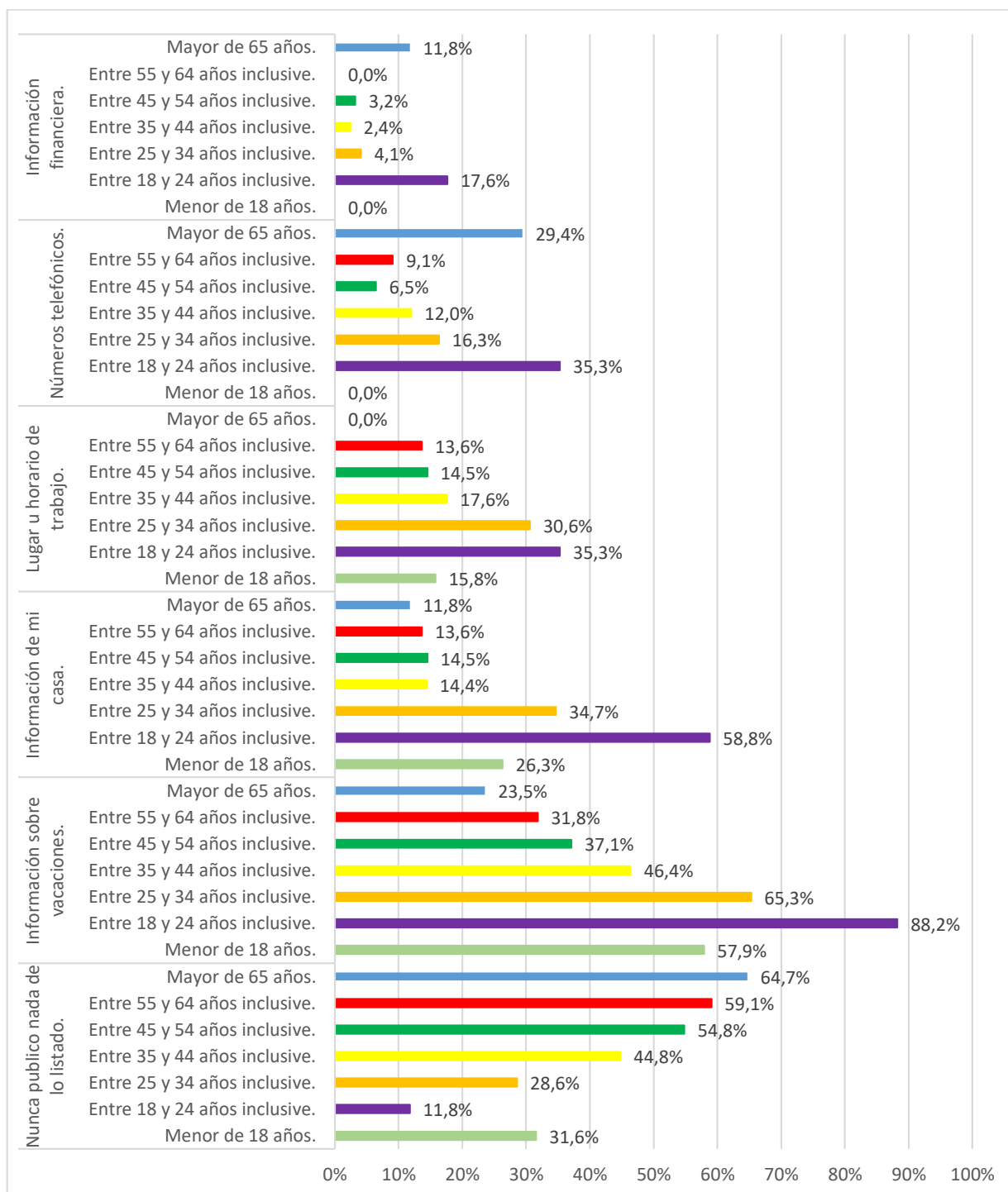


Gráfico 61: Publicación de información sensible, por edad (encuesta).

**Observaciones:**

- De la disgregación por edad, se desprende que son las personas “mayores” las que, en mayor proporción, han seleccionado la opción “Nunca publico nada de lo listado”. A su

vez, los porcentajes de encuestados que seleccionaron esta opción, disminuyen a medida que disminuye la edad del encuestado (a excepción de los menores de 18 años).

- Los encuestados que se encuentran en el rango de entre 18 y 24 años inclusive, son los que, en más altos porcentajes, dicen publicar información sobre todos los ítems preguntados. Seguidos en todos los casos por los encuestados de entre 25 y 34 años inclusive.
- A medida que se incrementa el rango etario, se observa una tendencia a la disminución de la cantidad de encuestados que dicen haber realizado publicaciones conteniendo información relacionada a cada tópico.

### PREGUNTA 6: ¿Cuáles de los siguientes datos considerarás privados?

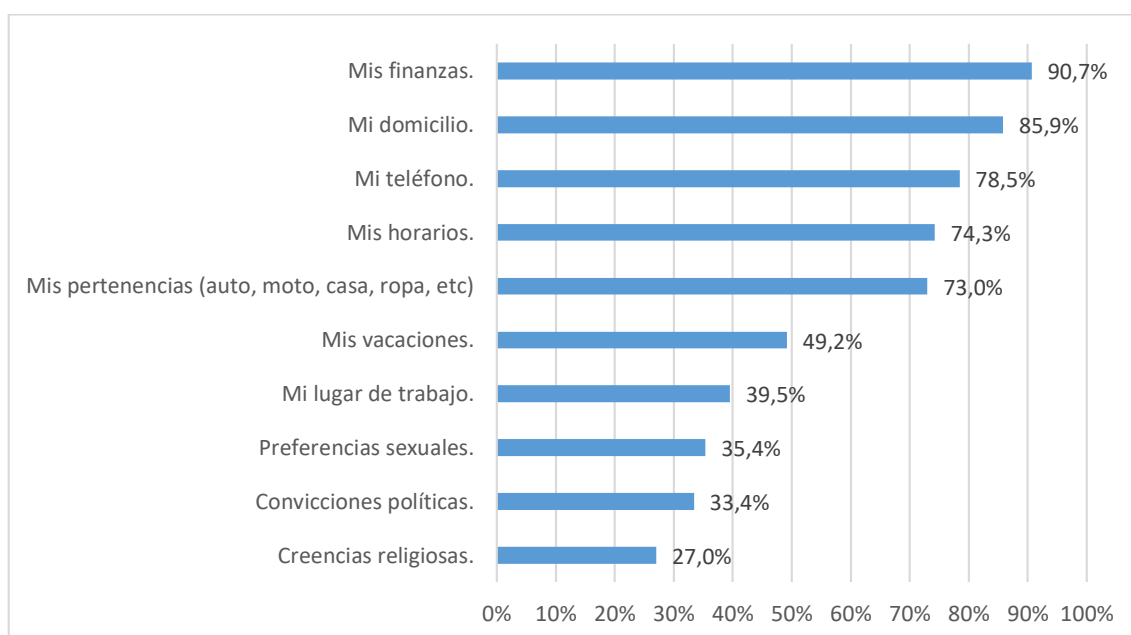


Gráfico 62: Información considerada privada (encuesta).

#### Observaciones:

- El domicilio es considerado como privado por un alto porcentaje de encuestados (85,9%).
- Información relacionada a “creencias religiosas”, “convicciones políticas” y “preferencias sexuales”, en general son las que en menor porcentaje han sido consideradas como privadas. Lo cual podría considerarse un dato llamativo hace no mucho tiempo atrás. En nuestro país, la gran cantidad de debate en cuanto a la ley de género, entre otras tantas discusiones, han llevado a una alta disminución en el cuidado

que se tiene respecto a proteger posturas adoptadas frente a las temáticas mencionadas.

Datos relacionados a información considerada privada disgregados por nivel de estudios:

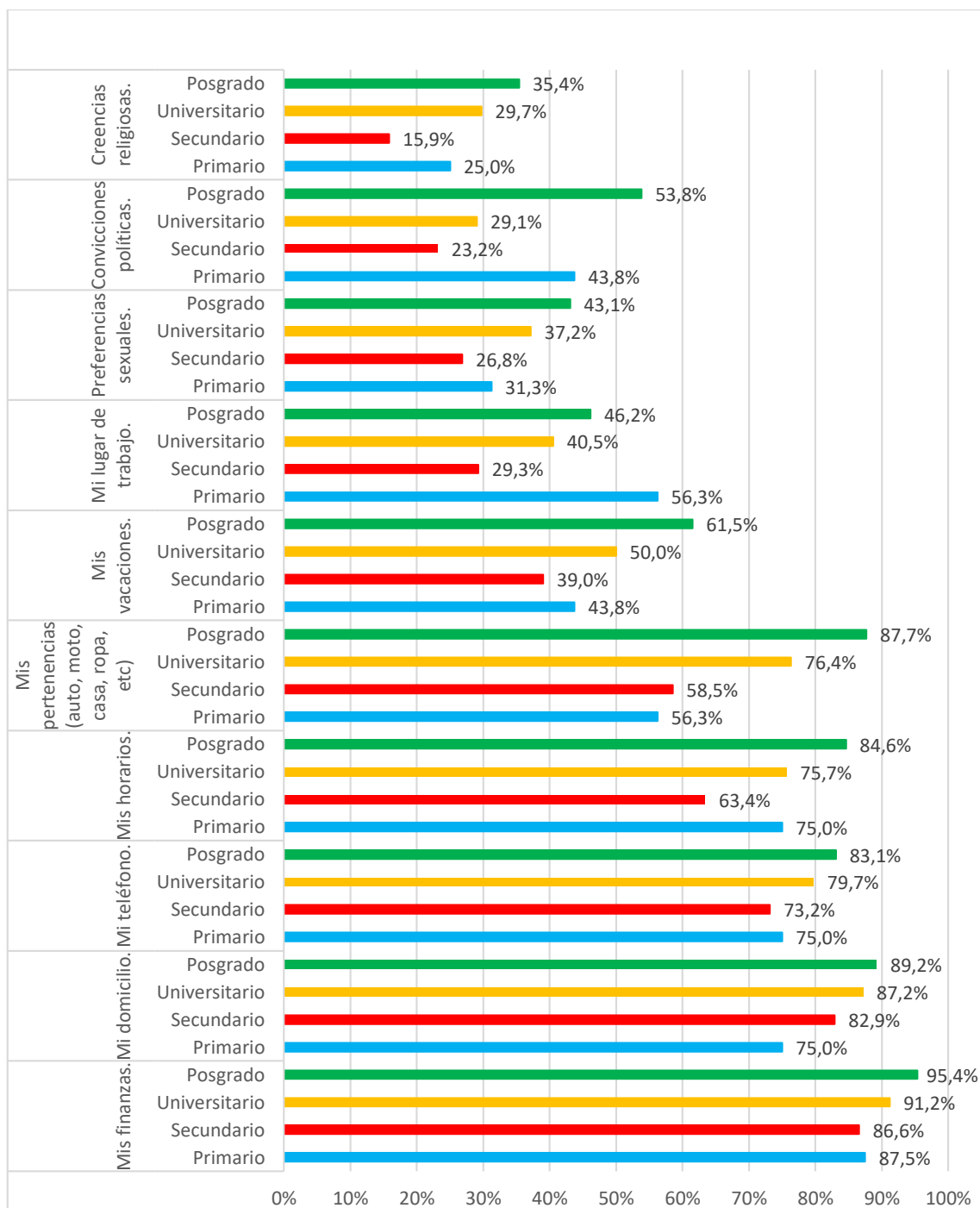


Gráfico 63: Información considerada privada, por nivel de estudios (encuesta).

**Observaciones:**

- En general, puede observarse una tendencia que, a mayor nivel de estudios, mayor el porcentaje de encuestados que consideran como privados los tópicos consultados.
- Notar que para varios casos, los encuestados con nivel de estudio “secundario”, representan los porcentajes menores. Es decir, los que en menor proporción consideran privados los temas abordados, incluso por debajo de los encuestados con estudio “primario”.

**PREGUNTA 7: ¿Tuviste la experiencia de publicar algo en las redes de lo cual te hayas arrepentido?**

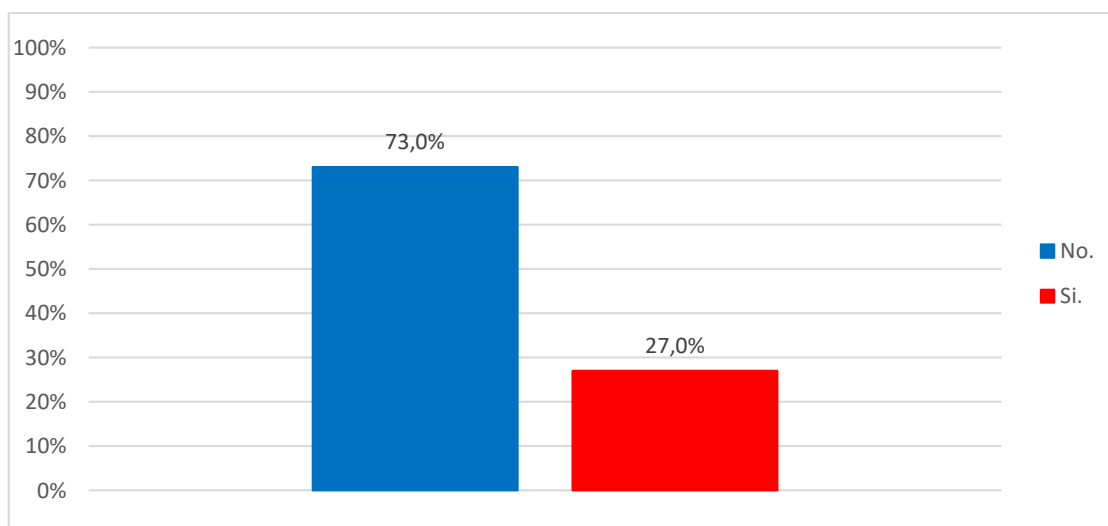


Gráfico 64: Arrepentimiento sobre lo publicado (encuesta).

Datos relacionados a la experiencia de publicar algo de lo cual se hayan arrepentido, disgregados por edad:

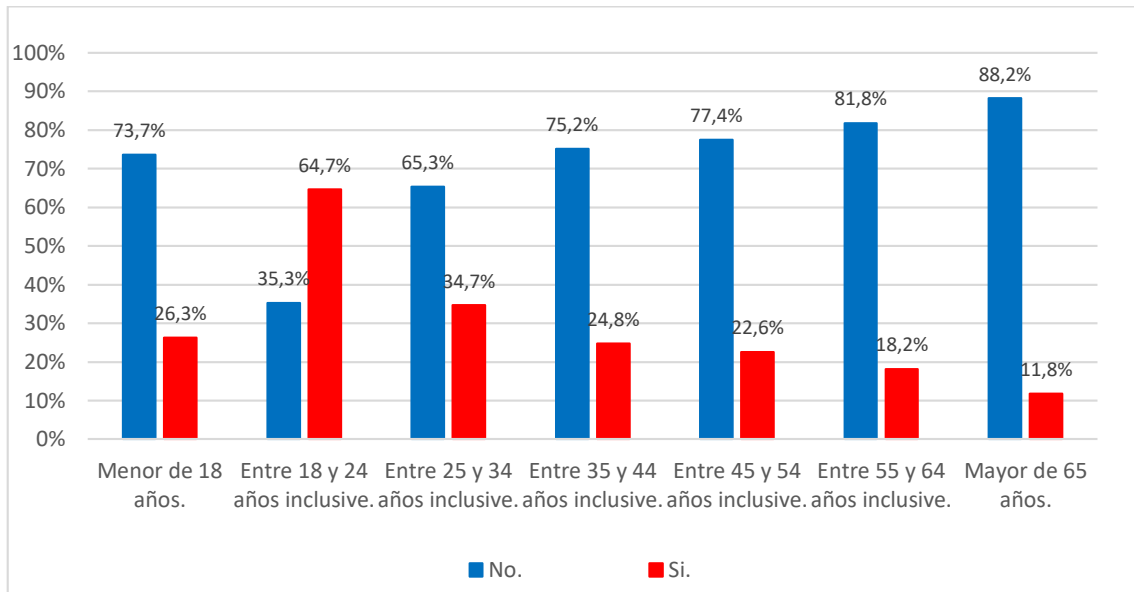


Gráfico 65: Arrepentimiento sobre lo publicado, por edad (encuesta).

#### Observaciones:

- Una observación interesante a partir del Gráfico 65, es que para todos los rangos etarios, la cantidad de encuestados que no publicaron cosas de las cuales se hayan arrepentido, supera ampliamente a aquellos que si les ha sucedido, a excepción del rango que va entre los 18 y 24 años inclusive, en el cual los que si se han arrepentido alguna vez superan ampliamente a los nunca lo han hecho. Sin duda esto caracteriza este particular rango etario.
- Por su parte, para el resto de los rangos etarios, se observa una leve tendencia a que la cantidad de encuestados que optaron por la respuesta “No” (no se arrepintieron de sus publicaciones) se vaya incrementando a medida que se incrementa la edad del encuestado. Es decir, cuantos más años tiene el encuestado, menor cantidad dicen haber publicado contenido del cual se ha arrepentido. Esto puede deberse a dos razones:
  - o La primera es que no realicen publicaciones con contenido sensible (podría estar relacionado a un menor volumen de información publicada).
  - o La segunda es que tienen menor conciencia de la criticidad o impacto de lo que publican, lo cual lleva a que no se arrepientan de haberlo publicado.



**PREGUNTA 8: ¿Facilitás la ubicación a aplicaciones de tu dispositivo móvil? (permite que las aplicaciones conozcan desde dónde te estás conectando)**

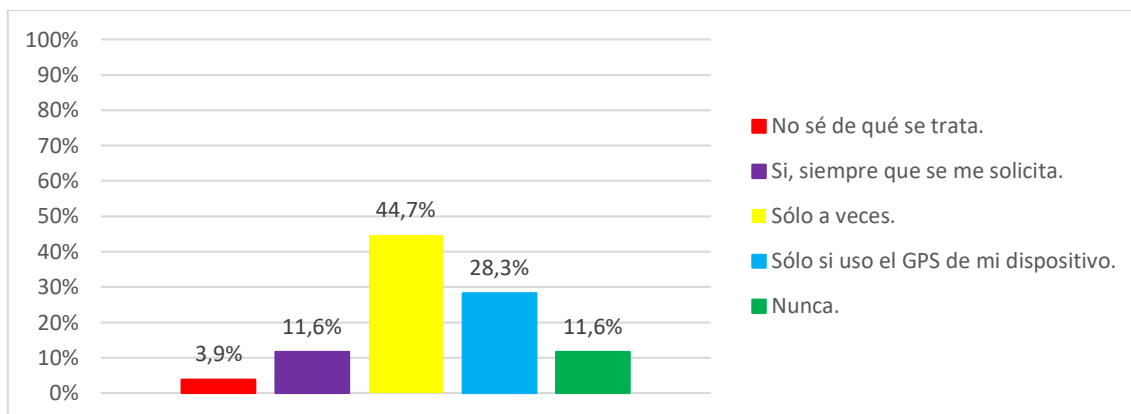


Gráfico 66: Uso de facilidades de geolocalización (encuesta).

**Observaciones:**

- El 3,9% dice no saber de qué se trata facilitar la ubicación a aplicaciones del dispositivo móvil. Es factible que un porcentaje de esos usuarios tengan habilitadas de manera permanente las funcionalidades de geolocalización, sin siquiera saberlo.
- Los encuestados que responden “Si, siempre que se me solicita” son el 11,6%. Se trata de un porcentaje alto de usuarios que seguramente tengan habilitada la funcionalidad de manera permanente, o casi permanente.
- Para el caso de los encuestados que responden “Sólo a veces”, se considera que son aquellos que lo habilitan, aun cuando no están empleando el GPS. Es decir, que lo habilitan a veces, más cuando usan el GPS. El porcentaje de los encuestados que seleccionaron esta opción, es de más del 44,7%.
- Es decir que sumando los ítems 2 (“Si, siempre que se me solicita”) y 3 (“Sólo a veces”), tenemos a más del 56% de los encuestados que mantienen habilitada la funcionalidad de geolocalización de su dispositivo móvil, aun cuando no están usando el GPS.
- Sólo el 11,6% dice no usar nunca las funcionalidades de geolocalización. Si a eso sumamos además, los que dicen “No sé de qué se trata”, ya que no se puede deducir si lo usan o no, aunque es probable que la funcionalidad se encuentre habilitada de manera permanente o casi permanente, tenemos que al menos el 84,3% (suma de las opciones 2, 3 y 4) las emplean con mayor o menor frecuencia.

Datos relacionados a la facilitación de la ubicación a las aplicaciones del dispositivo móvil, desgregados por edad:

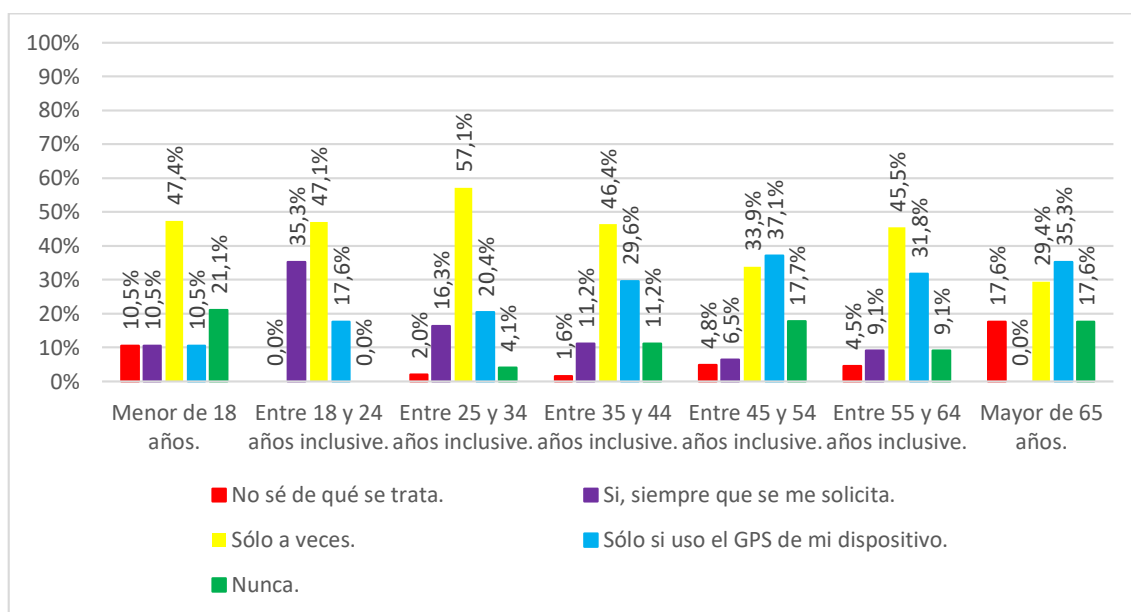


Gráfico 67: Uso de facilidades de geolocalización, por edad (encuesta).

#### Observaciones:

- Los encuestados que se encuentran en el rango de entre 18 y 24 años inclusive, son los que en mayor cantidad seleccionaron la respuesta “Si, siempre que se me solicita”. Es decir, que utilizan la geolocalización siempre que alguna aplicación en el dispositivo móvil así lo requiere.
- Por otro lado, se observa que los encuestados ubicados en los rangos etarios extremos (menores a 18 años, y mayores a 65 años), son los que en mayor proporción dicen no saber de qué se tratan las funciones de geolocalización. Para el caso de los mayores de 65 años, este porcentaje es elevado (17,6%).

**PREGUNTA 9: ¿Leíste o conocés la política de privacidad de las redes sociales que utilizás?**

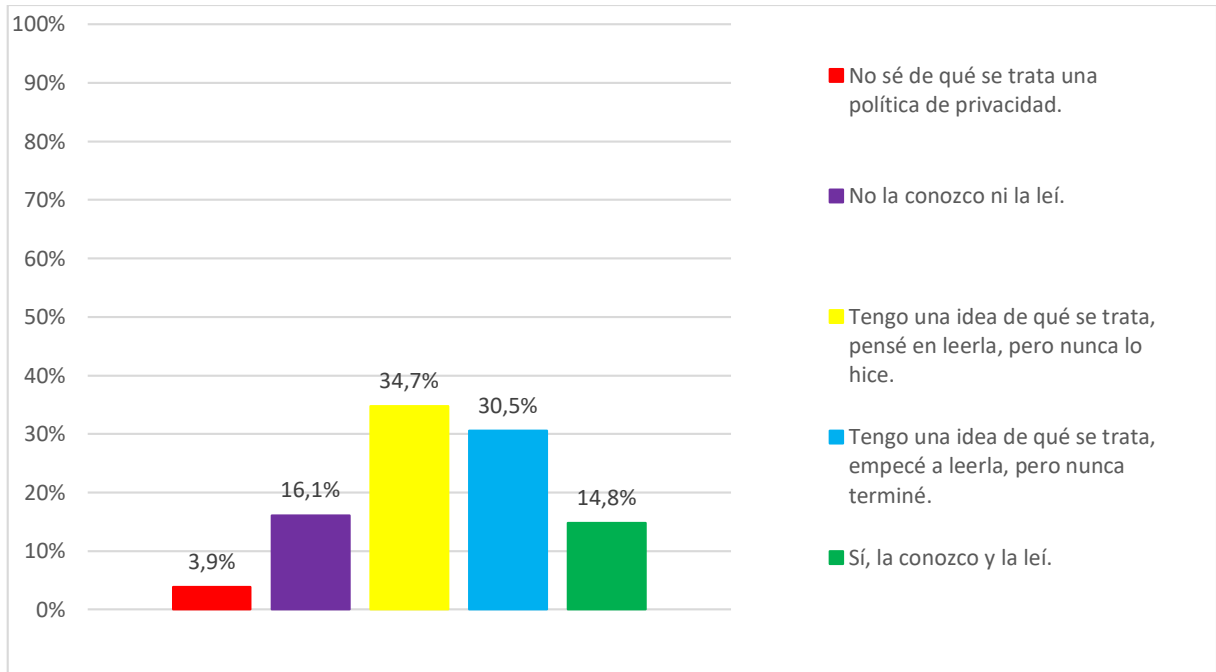


Gráfico 68: Conocimiento de políticas de privacidad (encuesta).

**Observaciones:**

- Sólo el 14,8% de los encuestados dice conocer y haber leído la política de seguridad de las redes sociales que emplean.
- El 3,9% de los encuestados desconoce de qué se trata una política de seguridad.
- El 16,1% de los encuestados, no la conocen ni la leyeron. Es decir que el 20% de los encuestados (suma de las opciones 1 y 2) desconoce absolutamente bajo qué condiciones hacen uso de las redes sociales que emplean.
- El resto de los encuestados (65,2% correspondientes a los porcentajes de las opciones 3 y 4 sumadas), tienen una idea de qué se trata, o bien comenzaron a leerla y no la terminaron. De más está decir que conocer o haber leído la política no significa que el usuario esté en contra de la misma, ya que el resultado final termina siendo la aceptación de las mismas, para el posterior uso de las bondades de la red.
- En total, más del 85% de los encuestados, nunca leyó la política de seguridad.

**PREGUNTA 10: ¿Personalizaste las opciones de privacidad de tu perfil en redes sociales? (Por ejemplo: quien puede o no ver tu contenido o comentar algo al respecto).**

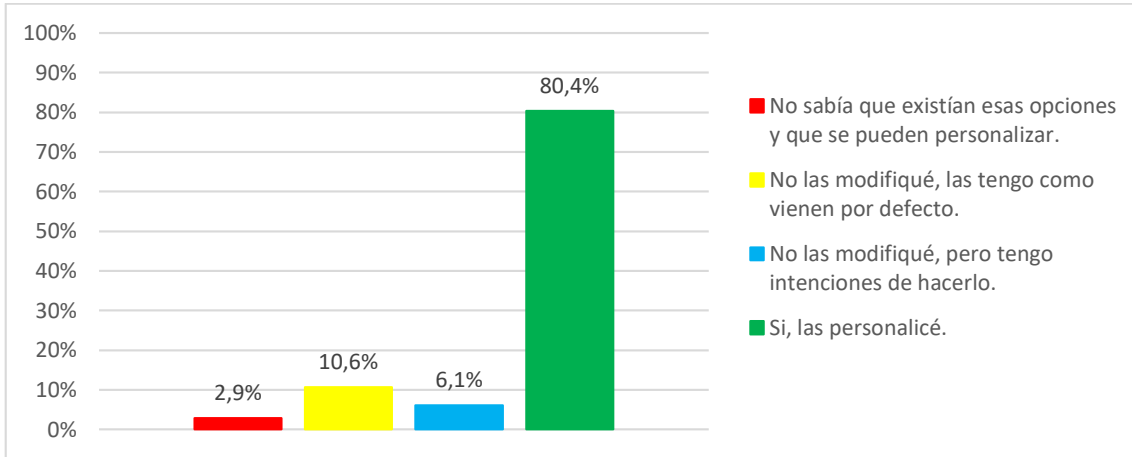


Gráfico 69: Personalización de configuración de privacidad (encuesta).

**Observaciones:**

- Más del 80% de los encuestados dice haber personalizado las opciones de privacidad de sus perfiles de redes sociales.
- El restante 20% no las modificó.

Datos relacionados a la personalización de las opciones de privacidad del perfil en redes sociales, disgregados por edad:

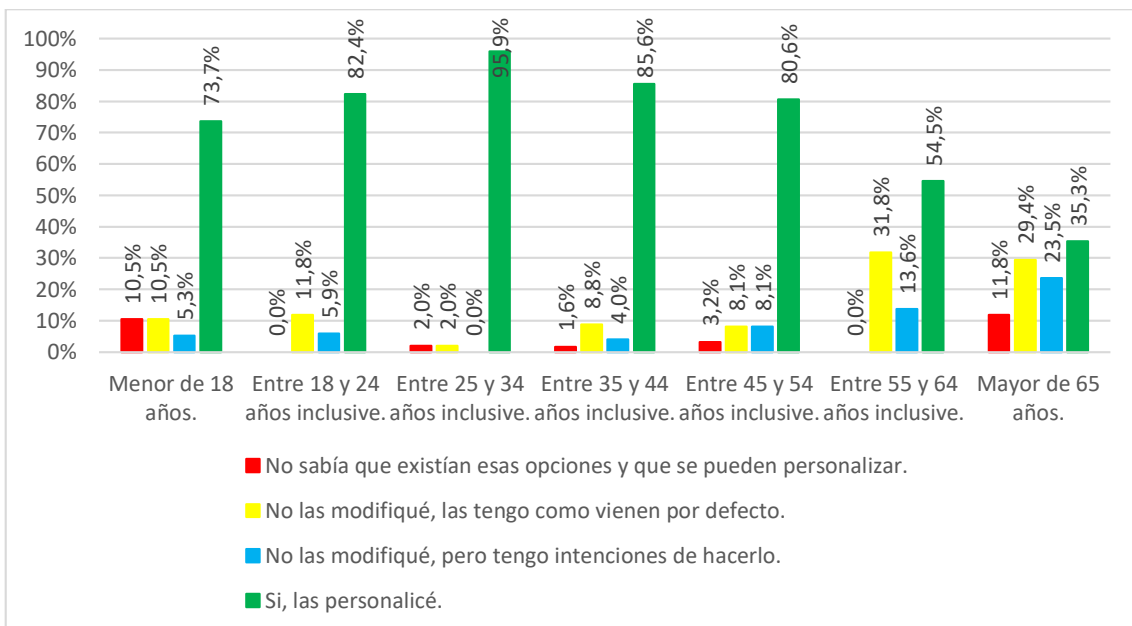


Gráfico 70: Personalización de configuración de privacidad, por edad (encuesta).

**Observaciones:**

- Los encuestados de entre 25 y 34 años inclusive son los que en mayor proporción (95,9%), dicen haber personalizado las opciones de configuración relacionadas a la privacidad.
- Los porcentajes disminuyen a medida que aumenta la edad del encuestado, y también a medida que la edad disminuye, dibujando una parábola.
- El porcentaje dentro de los encuestados mayores de 65 años que dice haber personalizado dichas opciones, es de tan sólo el 35,3%.
- También es bajo el porcentaje de encuestados que dice haber personalizado dichas opciones, que se encuentran en el rango de entre 55 y 64 años inclusive (54,5%).

**PREGUNTA 11: ¿Usás la misma contraseña para distintas aplicaciones?**

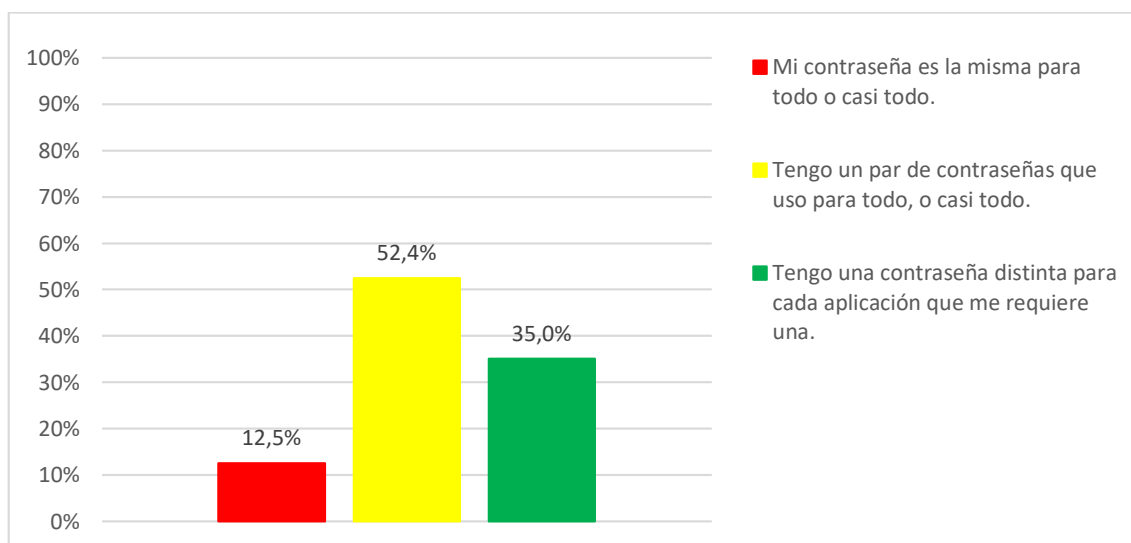


Gráfico 71: Uso de contraseñas (encuesta).

**Observaciones:**

- El 12,5% de los encuestados emplea la misma contraseña para todas las aplicaciones que usan.
- Sólo el 35% personaliza las contraseñas para cada aplicación. Es decir, posee una contraseña particular para cada aplicación que usa.
- La mayoría de los encuestados, tiene un conjunto de contraseñas que emplea para todo o casi todo.

Datos relacionados al uso de única/múltiples contraseñas, disgregados por edad:

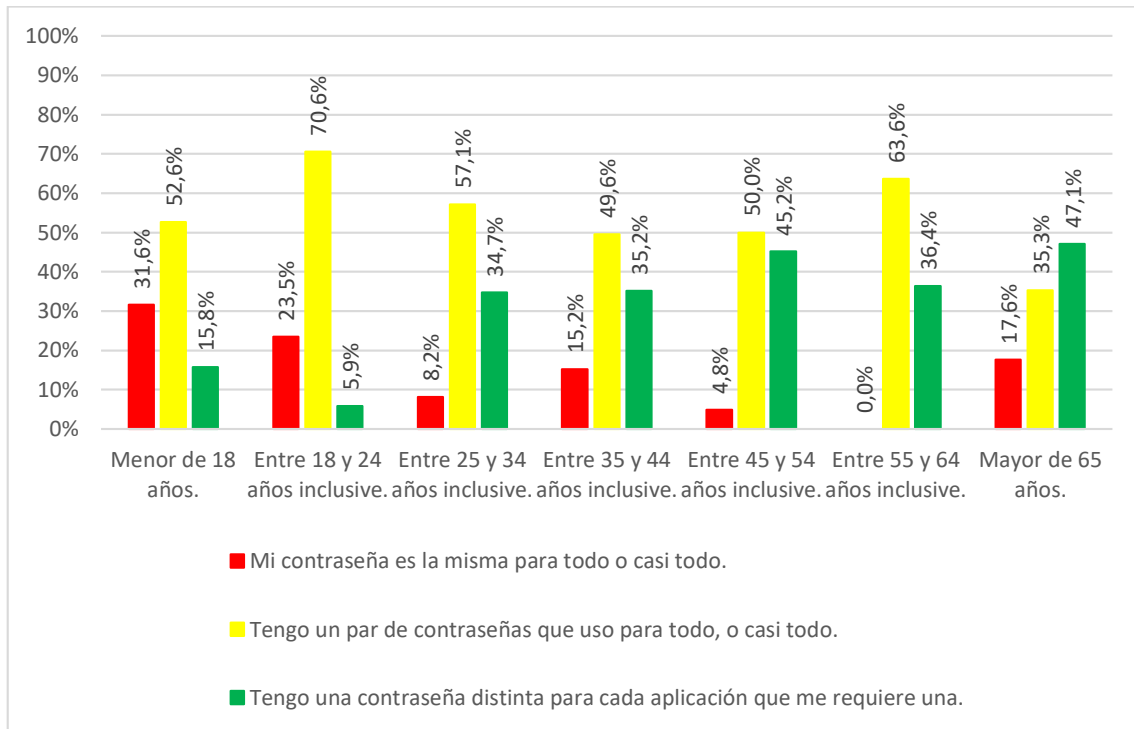


Gráfico 72: Uso de contraseñas, por edad (encuesta).

#### Observaciones:

- El rango etario con mayor porcentaje de encuestados que dice tener una contraseña para cada aplicación que utiliza, es el de mayores de 65 años. Esto se puede deber principalmente a dos factores:
  - o O bien un alto nivel de conciencia respecto a la temática.
  - o O bien hacen uso de pocas aplicaciones, lo que les permite mantener personalizadas las contraseñas.
- Los encuestados contenidos en los dos grupos etarios de menor edad (menores de 18 años, y entre 18 y 24 años inclusive), conforman los más altos porcentajes de usuarios que dicen emplear una única contraseña para todo o casi todo. Esto podría traducirse en un nivel bajo de concientización de los riesgos de llevar a cabo esa práctica.
- Notar que en el rango de encuestados de entre 18 y 24 años inclusive, el porcentaje de encuestados que tiene contraseñas distintas para cada aplicación, es de tan sólo el 5,9%. Esto podría deberse a la gran cantidad de aplicaciones que emplean, o bien a un bajo nivel de conciencia en la temática.

Datos relacionados al uso de única/múltiples contraseñas, disgregados por género:

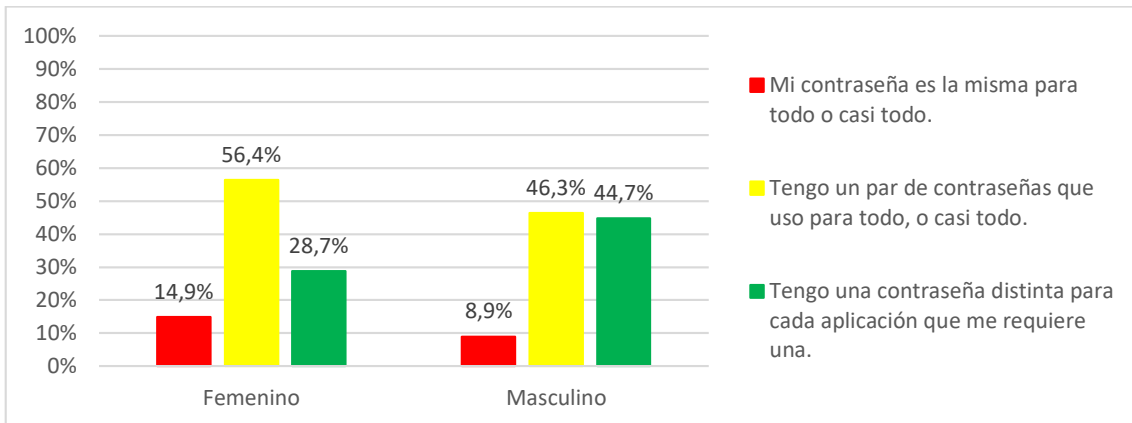


Gráfico 73: Uso de contraseñas, por género (encuesta).

**Observaciones:**

- Se observa una diferencia no menor (16 puntos porcentuales) a favor de los encuestados masculinos, de aquellos que dicen emplear una contraseña distinta para cada aplicación.
- A su vez, aunque con una diferencia menor, los encuestados masculinos son los que en menor proporción usan una única clave para todo o casi todo.

Datos relacionados al uso de única/múltiples contraseñas, disgregados por nivel de estudios:

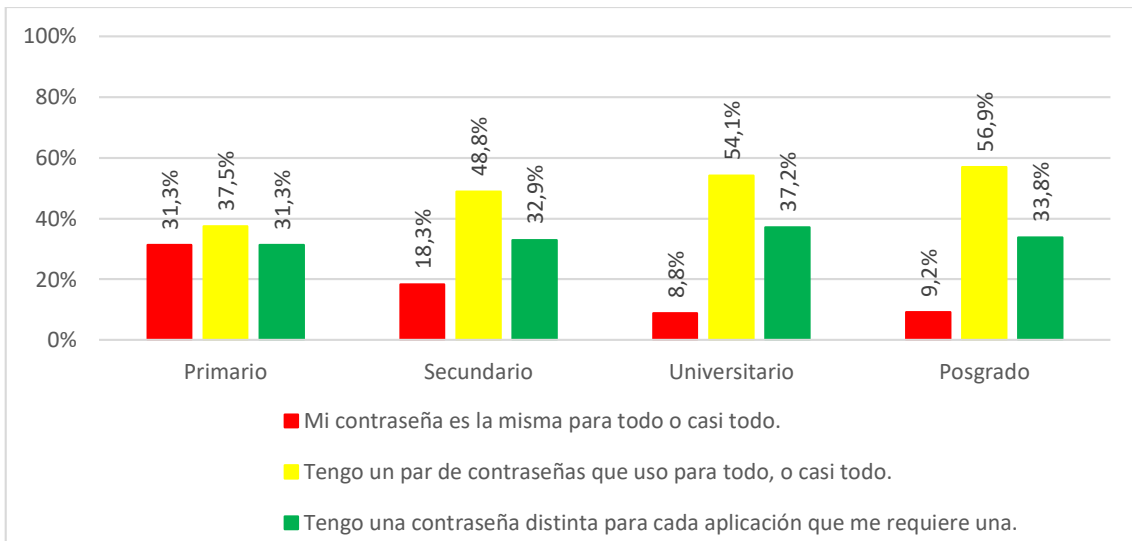


Gráfico 74: Uso de contraseñas, por nivel de estudios (encuesta).

**Observaciones:**

- Nótese que el porcentaje de encuestados que dice tener un par de contraseñas que usa para todo, o casi todo, se decrementa a medida que disminuye el nivel de estudios.

- De manera inversa a lo antes mencionado, el porcentaje de encuestados que dice tener la misma contraseña para todo, o casi todo, se decrementa a medida que aumenta el nivel de estudios.

**PREGUNTA 12: ¿Conocés a alguien que haya sufrido algún episodio de robo de información (robo de contraseña, robo de tarjetas de débito/crédito, etc)?**

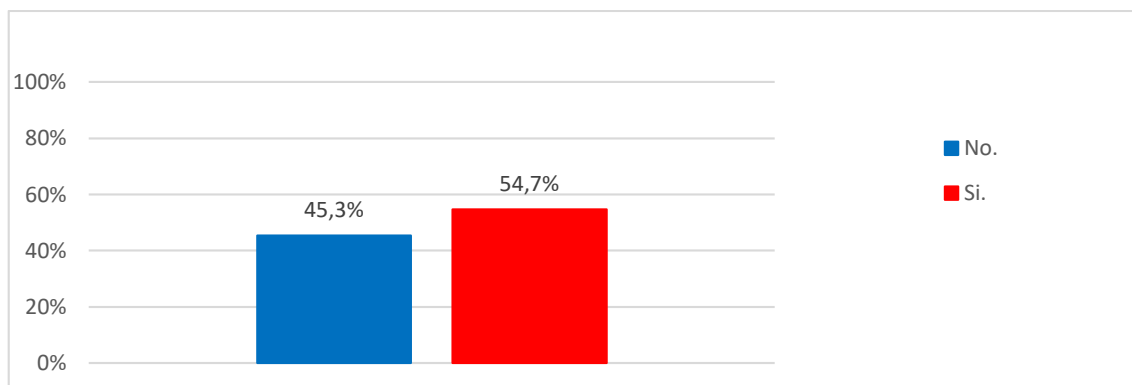


Gráfico 75: Conocimiento de robo de información (encuesta).

**Observaciones:**

- Más de la mitad de los encuestados conocen a alguien que sufrió robo de algún tipo de información (54,7%).

Datos relacionados al conocimiento de alguien que haya sufrido algún episodio de robo de información, disgregados por edad:

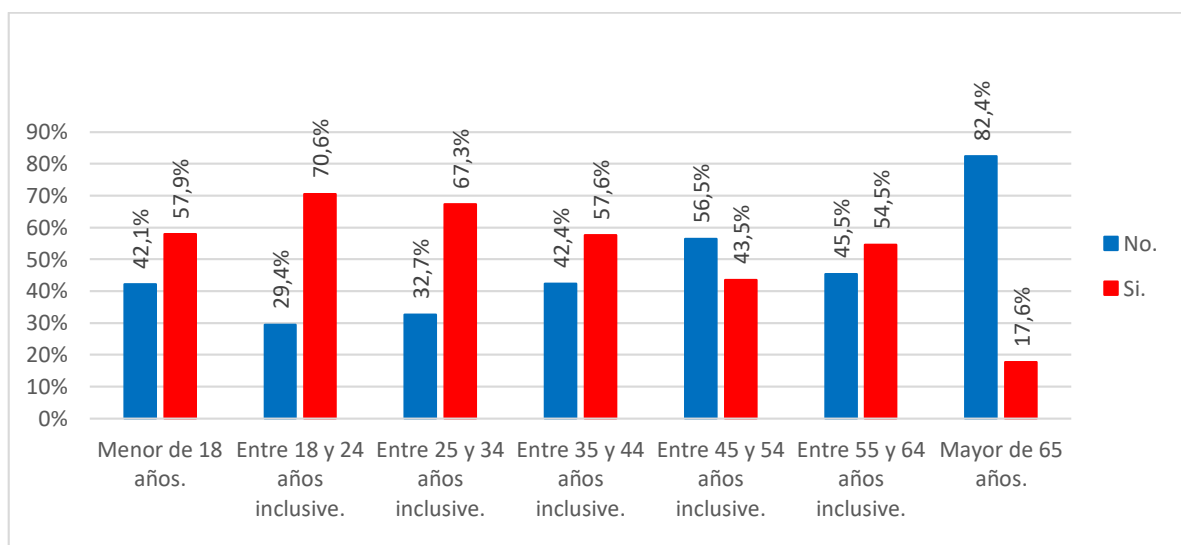


Gráfico 76: Conocimiento de robo de información, por edad (encuesta).



**Observaciones:**

- Nótese que los porcentajes más altos de encuestados que “Si” conoce gente que sufrió robo de información, se encuentra en el rango etario de entre 18 y 24 años inclusive (70,6%).
- Por el contrario, el porcentaje de encuestados más alto que “No” conoce gente que sufrió robo de información, se encuentra en el rango de mayores a 65 años.

**PREGUNTA 13: ¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)?**

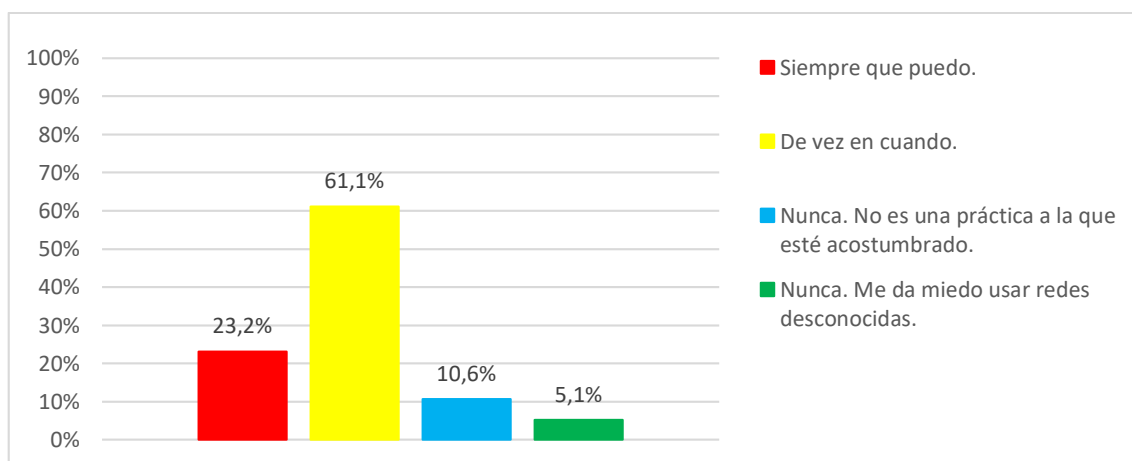


Gráfico 77: Uso de redes WiFi gratuitas (encuesta).

**Observaciones:**

- Sólo el 15,7% (suma de porcentajes correspondientes a las opciones 3 y 4) de los encuestados dice no usar nunca ese tipo de redes por alguna u otra razón.
- El resto, más del 84% (suma de porcentajes correspondientes a las opciones 1 y 2) hace uso de las mismas.

Datos relacionados al uso de redes WiFi gratuitas en la vía pública, disgregados por edad:

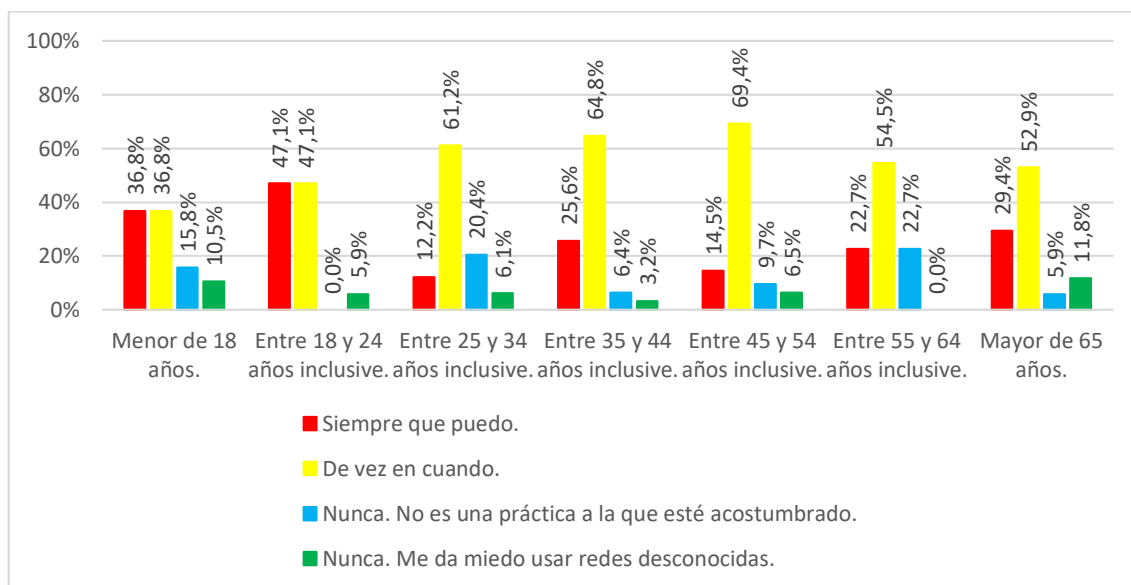


Gráfico 78: Uso de redes WiFi gratuitas, por edad (encuesta).

#### Observaciones:

- Lo encuestados ubicados en el rango de entre 18 y 24 años inclusive, son los que en mayor proporción y con notable diferencia, hacen uso de las redes gratuitas con 94,2% (si sumamos los porcentajes correspondientes a las dos primeras opciones de respuesta). Nótese la diferencia respecto del resto de los grupos etarios (a excepción de los encuestados ubicados en el rango de entre 35 y 44 años inclusive que, con 90,4%, lo separan poco menos de 5 puntos porcentuales).
- Los mayores de 65 años, son los que en mayor medida eligieron la opción “Nunca, me da miedo usar redes desconocidas”. Pero aun así, con tan sólo 11,8% de los encuestados. Para el resto de los grupos etarios, la selección de esta opción es llamativamente baja.

Datos relacionados al uso de redes WiFi gratuitas en la vía pública, disgregados por nivel de estudios:

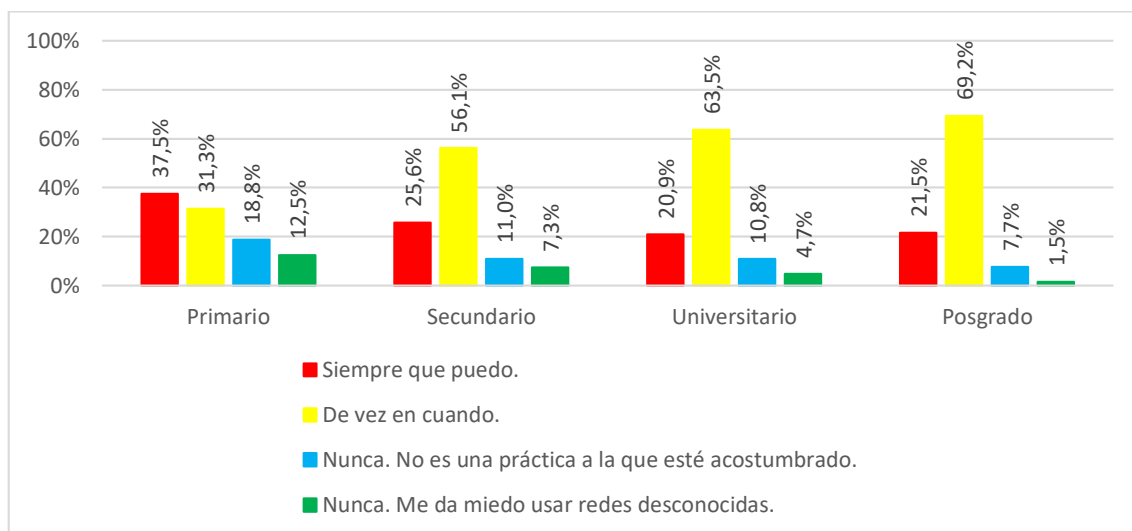


Gráfico 79: Uso de redes WiFi gratuitas, por nivel de estudios (encuesta).

#### Observaciones:

- Nótese que para la opción “Siempre que puedo”, el porcentaje tiende a disminuir a medida que aumenta el nivel de estudios (con una leve caída en el nivel universitario frente al nivel de posgrado). Esto podría llevarnos a concluir que, a mayor nivel de estudios, menos uso de redes WiFi de manera imperiosa. Pero a su vez, esto se contradice con lo que se visualiza con la selección de la opción “De vez en cuando”, la cual crece en porcentaje a medida que aumenta el nivel de estudios. Por lo cual, concluir que a mayor nivel de estudios, menor uso de redes WiFi públicas, no es del todo cierto.
- Con respecto a la opción “Nunca...” en cualquiera de sus dos alternativas. El porcentaje tiende a disminuir a medida que aumenta el nivel de estudios. Esto también contradice la suposición que la conciencia en el uso de este tipo de redes aumenta con el nivel de estudios.

**PREGUNTA 14: ¿Tenés conocimiento de los datos acerca de tu vida cotidiana que recolecta Google?**

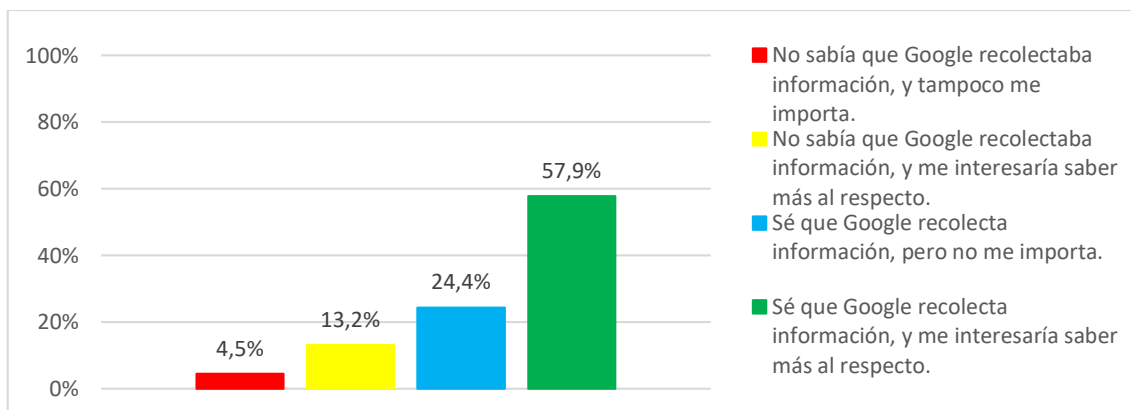


Gráfico 80: Conocimiento recolección de datos Google (encuesta).

**Observaciones:**

- El porcentaje de encuestados que no sabía sobre la recolección de datos por parte de Google (suma de por porcentajes correspondientes a las opciones 1 y 2) es del 17,7%.
- El porcentaje de encuestado que no le importa el hecho que Google recolecte información, independientemente de si lo sabían o no (suma de los porcentajes correspondientes a de las opciones 1 y 3) es del 28,9%. Es decir, más de la cuarta parte de los encuestados.

Datos relacionados al conocimiento de la recolección de datos por parte de Google, disgregados por edad:

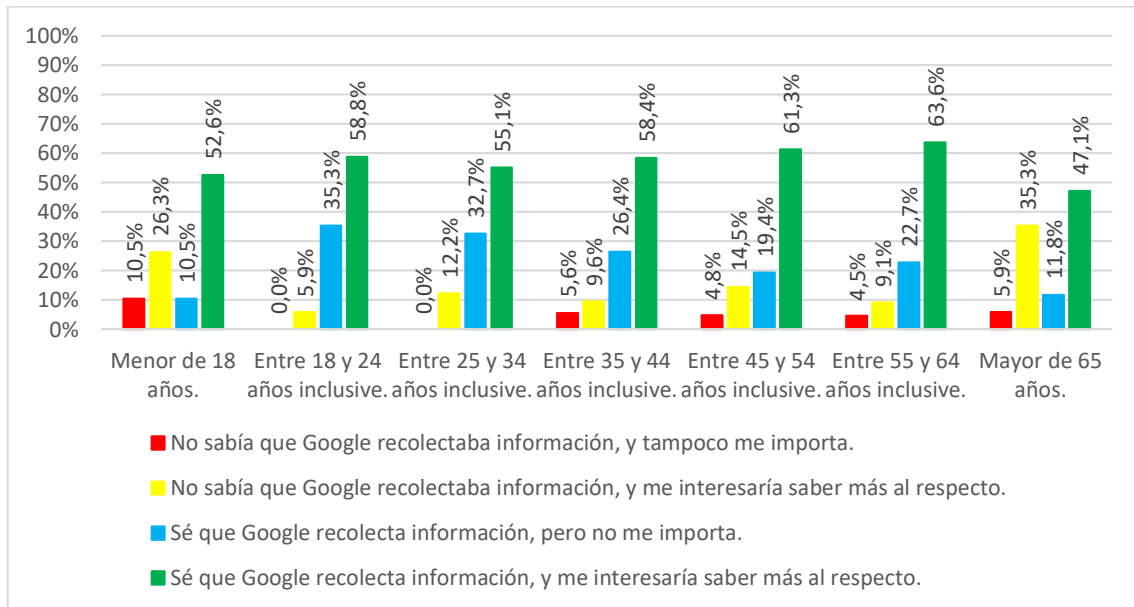


Gráfico 81: Conocimiento recolección de datos Google, por edad (encuesta).

#### Observaciones:

- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 2, se obtiene el porcentaje total de encuestados que dicen no saber sobre la recolección de información por parte de Google:
  - o Menor de 18 años => 36,8%
  - o Entre 18 y 24 años inclusive => 5,9%
  - o Entre 25 y 34 años inclusive => 12,2%
  - o Entre 35 y 44 años inclusive => 15,2%
  - o Entre 45 y 54 años inclusive => 19,3%
  - o Entre 55 y 64 años inclusive => 13,6%
  - o Mayores de 65 años => 41,2%
- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 3, se obtiene el porcentaje total de encuestados que dicen que no les importa sobre la recolección de información por parte de Google:
  - o Menor de 18 años => 21%
  - o Entre 18 y 24 años inclusive => 35,3%
  - o Entre 25 y 34 años inclusive => 32,7%
  - o Entre 35 y 44 años inclusive => 32%
  - o Entre 45 y 54 años inclusive => 24,2%

- Entre 55 y 64 años inclusive => 27,2%
- Mayores de 65 años => 17,7%

Datos relacionados al conocimiento de la recolección de datos por parte de Google, disgregados por género:

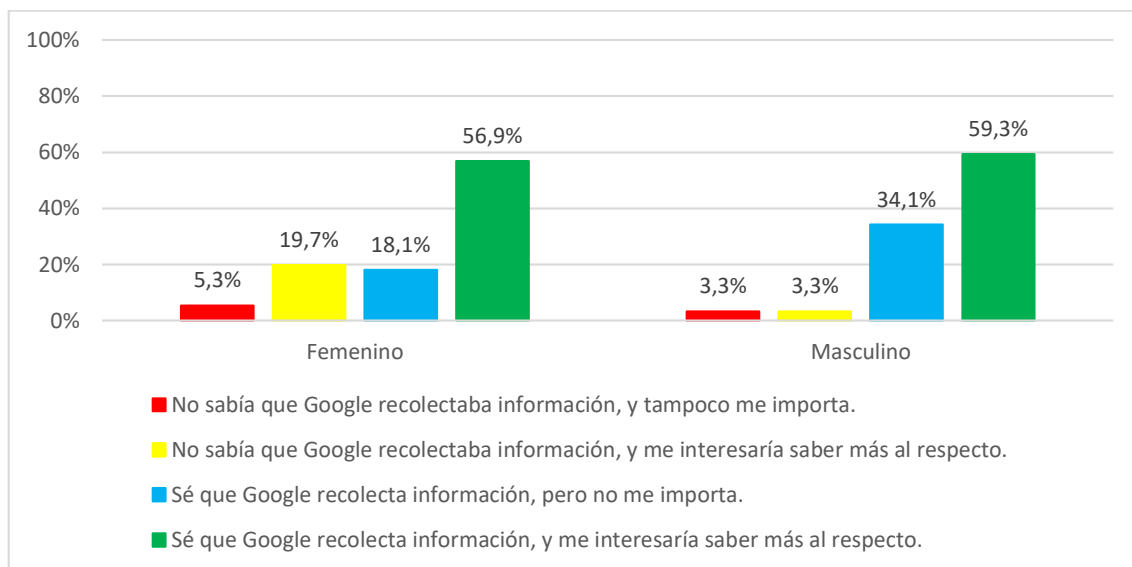


Gráfico 82: Conocimiento recolección de datos Google, por género (encuesta).

#### Observaciones:

- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 2, se obtiene el porcentaje total de encuestados que dicen no saber sobre la recolección de información por parte de Google:
  - Femenino => 25%
  - Masculino => 6,6%
- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 3, se obtiene el porcentaje total de encuestados que dicen que no les importa sobre la recolección de información por parte de Google:
  - Femenino => 23,4%
  - Masculino => 37,4%

Datos relacionados al conocimiento de la recolección de datos por parte de Google, disgregados por nivel de estudios:

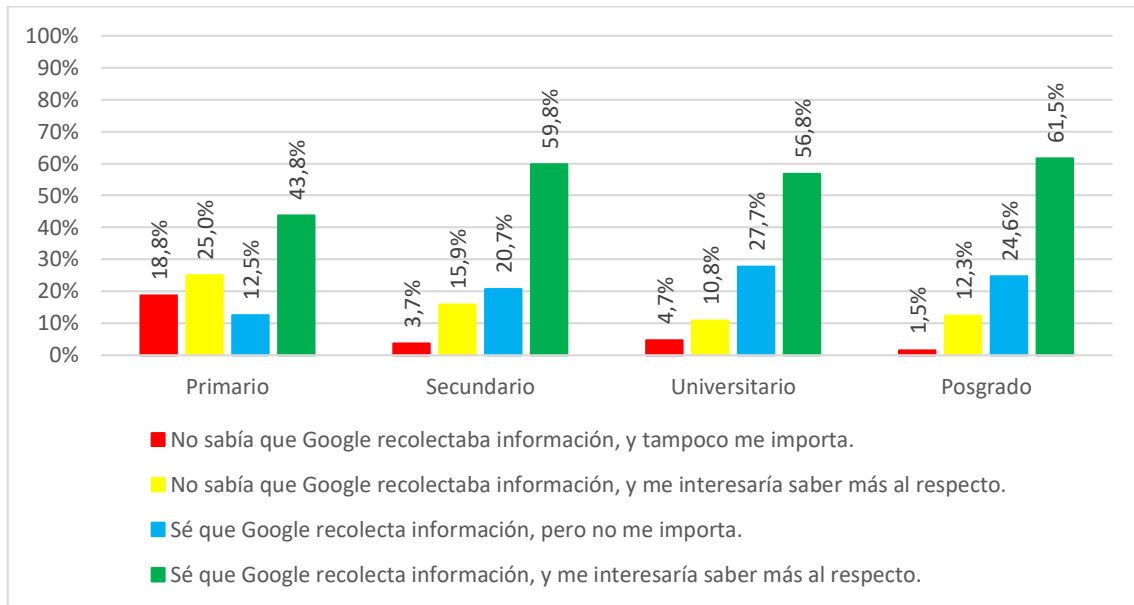


Gráfico 83: Conocimiento recolección de datos Google, por nivel de estudios (encuesta).

#### Observaciones:

- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 2, se obtiene el porcentaje total de encuestados que dicen no saber sobre la recolección de información por parte de Google:
  - Primario => 43,8%
  - Secundario => 19,6%
  - Universitario => 15,5%
  - Posgrado => 13,8%
- Si se suman los porcentajes correspondientes a las alternativas 1, con los de la alternativa 3, se obtiene el porcentaje total de encuestados que dicen que no les importa sobre la recolección de información por parte de Google:
  - Primario => 31,3%
  - Secundario => 24,4%
  - Universitario => 32,4%
  - Posgrado => 26,1%

**PREGUNTA 15: ¿Qué pensás sobre la instalación de cámaras de video en la vía pública, y en la posibilidad que las mismas graben parte de nuestra vida diaria?**

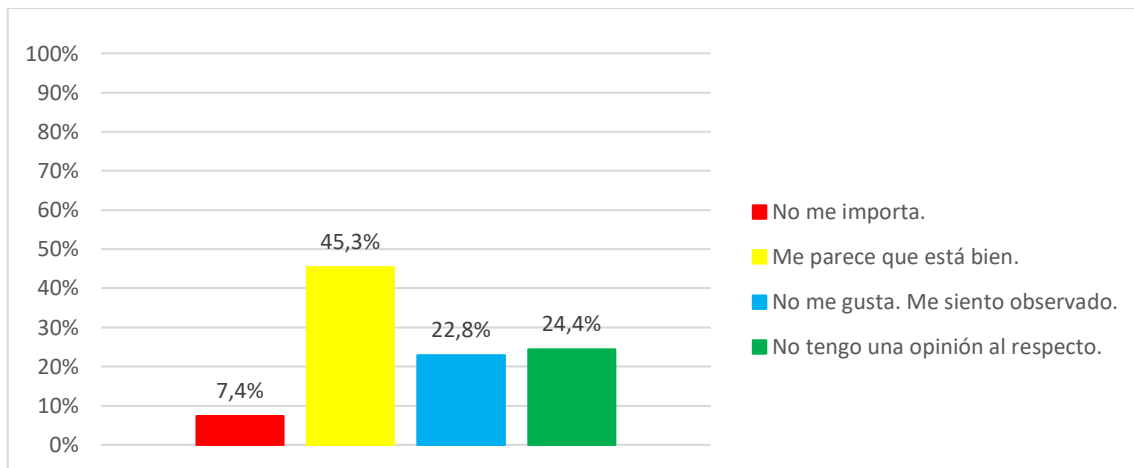


Gráfico 84: Opinión cámaras de seguridad (encuesta).

**Observaciones:**

- El porcentaje de encuestados que manifiesta desacuerdo con la instalación de cámaras por sentirse observado, es del 22,8%.
- Los porcentajes correspondientes a los ítems 1 (“No me importa”), 2 (“Me parece que está bien”) y 4 (“No tengo una opinión al respecto”) sumados, resultarían aquellos encuestados que a priori, no consideran que la instalación de cámaras en la vía pública sea un potencial riesgo para su privacidad. Esta suma alcanza el 77,1% del total de los encuestados.

Con respecto a la pregunta número 12 (“¿Conocés a alguien que haya sufrido algún episodio de robo de información?”) resulta de interés llevar a cabo un análisis un poco más profundo. El mismo pretende conocer si el hecho de conocer a alguien que haya sufrido algún episodio de robo de información, condiciona a que el encuestado presente algún cambio de comportamiento ante determinadas cuestiones consultadas en el resto de las preguntas de la encuesta. Las preguntas analizadas son:

- Pregunta 5: ¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems?
- Pregunta 6: ¿Cuáles de los siguientes datos considerás privados?
- Pregunta 8: ¿Facilitás la ubicación a aplicaciones de tu dispositivo móvil?
- Pregunta 9: ¿Leíste o conocés la política de privacidad de las redes sociales que utilizás?
- Pregunta 10: ¿Personalizaste las opciones de privacidad de tu perfil en redes sociales?



- Pregunta 11: ¿Usás la misma contraseña para distintas aplicaciones?
- Pregunta 13: ¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)?
- Pregunta 14: ¿Tenés conocimiento de los datos acerca de tu vida cotidiana que recolecta Google?
- Pregunta 15: ¿Qué pensás sobre la instalación de cámaras de video en la vía pública, y en la posibilidad que las mismas graben parte de nuestra vida diaria?

Lo que se hizo, es analizar la respuesta de los encuestados a las preguntas antes listadas, pero discriminando, por un lado para aquellos que respondieron “Si” a la pregunta 12 (es decir que SI conocen a alguien que haya sufrido un episodio de robo de información), y por otro lado aquellos que respondieron que “No” a la misma pregunta 12. La intención era analizar si se observa algún tipo de desviación en las respuestas, con ese condicionante.

El detalle de dicho análisis con los gráficos asociadas, no fueron incluidos dentro del presente documento, ya que del mismo no se obtuvo ninguna conclusión determinante. Es decir que el hecho de tener conocidos que hayan sufrido robos de información, no lleva a las personas a ser más precavidas o cuidadosas a la hora de usar las TICs.

Otro análisis llevado a cabo, involucra los datos representados a través del Gráfico 60, correspondientes a la pregunta 5 (“¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems?”). A simple vista, dicho gráfico, pareciera demostrar un alto nivel de conciencia en la temática abordada, en al menos el 43,7% de los encuestados que responden “Nunca publico nada de lo listado”. Por tal razón, se decidió hacer un análisis puntual sobre ese 43,7%, de manera de determinar si dichos encuestados respondieron de tal forma porque son conscientes de los riesgos asociados a publicar información como la consultada, o bien por alguna otra razón distinta que a priori no está relacionada con el conocimiento de dichos riesgos. Se toma como referencia la Pregunta 13 (“¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)?”) y se evalúa qué respuesta dieron los encuestados incluidos en ese 43,7%, y el resultado es que se ilustra a continuación a través del Gráfico 85:

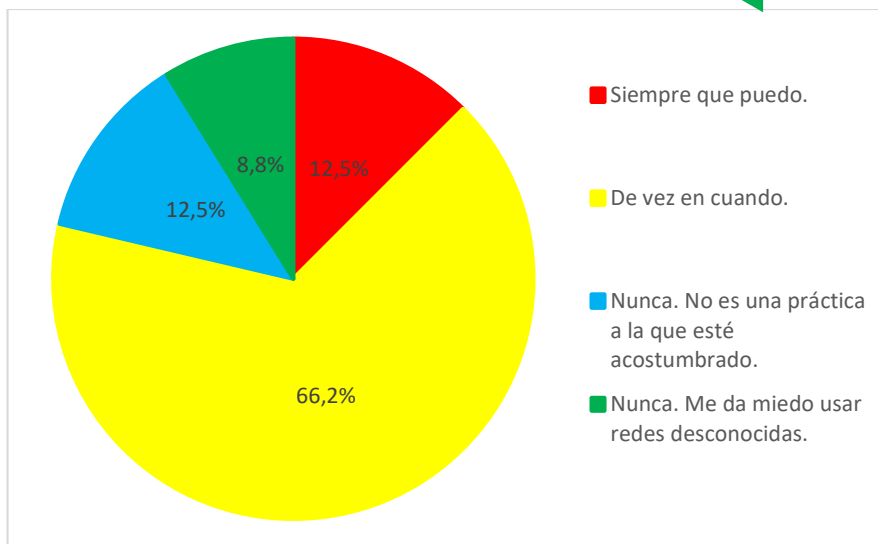
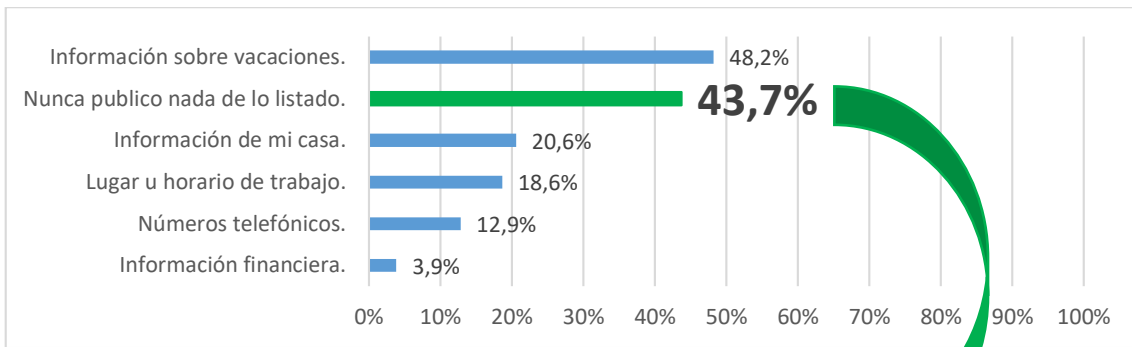


Gráfico 85: Análisis de los que “Nunca publican nada” (encuesta).

Del gráfico se desprende que el 21,3% (obtenido a partir de sumar los porcentajes correspondientes a las opciones “Nunca. No es una práctica...” y “Nunca. Me da miedo...” ) del subuniverso de 43,7% sobre el cual se está haciendo el análisis, responde que nunca usa redes WiFi gratuitas. El 88,7% restante lo hace, con todos los riesgos que ello implica tal como se explica en los artículos de WeLiveSecurity (Riesgos asociados a las redes Wi-Fi públicas - ESET, 2019) y de Infobae (Jaimovich, 2019).

Esto se hace para descartar que este subuniverso analizado, responde no publicar contenido como el consultado a través de la pregunta 5, no por conocimiento o conciencia de los riesgos, sino por alguna otra razón que excede este análisis. Es decir que menos del 10% de la muestra total de encuestados (que sería lo mismo que decir el 21,3% del 43,7% de la muestra total), son los que además de no publicar nada de lo consultado a través de la pregunta 5, no hacen uso de redes WiFi gratuitas (independientemente de la razón). Es decir, que sólo ese 10% podría decirse que muestra cierta conciencia en la combinación de esas dos preguntas.

Como último análisis a realizar sobre las respuestas obtenidas, se toman aquellos encuestados que respondieron las preguntas de manera tal que se pueda inferir el seguimiento de buenas prácticas en el uso de TICs.

En primera instancia se evalúan como buenas prácticas básicas, a la hora de usar TICs las siguientes:

- El hecho de no publicar en las redes sociales, información que podría considerarse sensible.
- Haber personalizado las opciones de configuración de privacidad del perfil de redes sociales empleadas.
- No emplear la misma contraseña para todas las aplicaciones.
- No usar redes WiFi gratuitas.

Es decir, se analizan las preguntas que se detallan en el cuadro siguiente bajo la columna “Pregunta Analizada, y se buscan las respuestas detalladas bajo la columna “Respuestas buscadas”.

#Pregunta	Pregunta Analizada	Respuestas buscadas
5	¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems?	Nunca publico nada de lo listado.
10	¿Personalizaste las opciones de privacidad de tu perfil en redes sociales?	Si, las personalicé.
11	¿Usás la misma contraseña para distintas aplicaciones?	Tengo una contraseña distinta para cada aplicación que me requiere una.
		Tengo un par de contraseñas que uso para todo, o casi todo.
13	¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)?	Nunca. Me da miedo usar redes desconocidas.
		Nunca. No es una práctica a la que esté acostumbrado.
<b>Resultado: 7,9%</b>		

Sólo el 7,9% del total de los encuestados han respondido la encuesta siguiendo las pautas descriptas en el cuadro anterior.

Si se busca un poco más de exigencia en el cumplimiento de las buenas prácticas (mínimas), incorporando que además de lo anterior, el encuestado tenga una idea de lo que se trata la política de privacidad de las redes sociales que utiliza (que las haya leído, o bien que al menos haya empezado a leerlas). El cuadro de las preguntas analizadas y respuestas buscadas sería:

# Pregunta	Pregunta Analizada	Respuestas buscadas
5	¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems?	Nunca publico nada de lo listado
9	¿Leíste o conocés la política de privacidad de las redes sociales que utilizás?	Sí, la conozco y la leí.
		Tengo una idea de qué se trata, empecé a leerla, pero nunca terminé.
10	¿Personalizaste las opciones de privacidad de tu perfil en redes sociales?	Si, las personalicé.
11	¿Usás la misma contraseña para distintas aplicaciones?	Tengo una contraseña distinta para cada aplicación que me requiere una.
		Tengo un par de contraseñas que uso para todo, o casi todo.
13	¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)?	Nunca. Me da miedo usar redes desconocidas.
		Nunca. No es una práctica a la que esté acostumbrado.
<b>Resultado: 4,4%</b>		

Sólo el 4,4% del total de encuestados ha respondido la encuesta siguiendo el patrón deseado que se detalla en el último cuadro.

## Conclusiones

### Uso de redes Sociales, y datos sensibles

- El uso de múltiples redes sociales, es una práctica instalada en un alto porcentaje de encuestados. Tan sólo el 0,3% no emplea ninguna red social (Gráfico 57).
- El 54,3% publica material sensible. Para el 45,7% restante que dice no hacerlo (al menos sobre el material consultado), se observa que más del 79% usa redes WiFi gratuitas.
- Distintas redes sociales se asocian de manera notable al rango etario de los usuarios que las emplean. Es decir, que su uso es bien marcado para distintos grupos etarios. Esto significa que dependiendo el rango de edad sobre el cual se desee hacer foco con algún tipo de comunicación o mensaje que se quiera hacer llegar, se puede elegir una red social específica para aumentar las probabilidades de éxito (Gráfico 58 y Gráfico 59).
- Más de la mitad de los encuestados, han manifestado publicar en sus redes sociales, contenido que podría llegar a considerarse como sensible (Gráfico 60). Pero a la vez, también casi la mitad de los encuestados, reconoce que ciertos tópicos incluidos en el gráfico anterior, son considerados privados (Gráfico 62). Esto denota una contradicción entre lo que publican, y lo que dicen considerar privado. O bien, lleva a concluir que, aun siendo información privada, eso no es condición suficiente como para no ser publicada. A continuación, en formato tabla se presentan los datos para una fácil lectura y comparación sobre en análisis de esta “contradicción”:

Información relacionada a:	Publicó (%)	Considera Privado (%)
Vacaciones	48,2	49,2
Casa	20,6	73
Trabajo	18,6	39,5
Números telefónicos	12,9	78,5

En la tabla anterior, puede leerse que el 48,2% de los encuestados publicó información relacionada a sus vacaciones, y a la vez, el 49,2% del total de encuestados, considera privada la información asociada a sus vacaciones.

- Casi el 86% de los encuestados considera el domicilio como algo privado (Gráfico 62). Sin embargo, este dato puede ser publicado por cualquiera, incluso sin nuestro consentimiento tal como se estipula en el artículo 5 de la Ley 25.326 (Protección de los Datos Personales de nuestro país que es la que regula actualmente en la materia):

“No será necesario el consentimiento cuando:

..... Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio”

A su vez, y tal como se explica en el ANEXO III de este documento, titulado “¿Qué sabe Google de mí?”, Google es capaz de deducir cuál es nuestro domicilio en base a determinada información recolectada del uso de nuestros dispositivos móviles, entre otras cosas. Por lo cual, lo que la mayoría de los encuestados considera como un dato privado, puede ser conocido, incluso sin que nunca hayamos brindado precisión al respecto. Esto significa que la información del domicilio (seleccionada por gran cantidad de encuestados como de las consideradas privadas) es fácilmente manipulable y fácil de obtener por cualquier tercero que así lo desee.

- El 27% de los encuestados (más de uno cada cuatro encuestados), ha publicado cosas de las cuales se ha arrepentido luego (Gráfico 64). Todo lo que se publica, queda en la red. Nunca desaparece. Sin duda estos números hablan a las claras de la importancia de pensar dos veces antes de publicar un contenido, y de fortalecer la relevancia del concepto de la perdurabilidad del mismo en el ciber espacio.

#### Uso de las funcionalidades de geolocalización

- Más del 84% de los encuestados las emplea con mayor o menor frecuencia (Gráfico 66). Esto significa que más de 8 de cada 10 encuestados suministran información a través de esta funcionalidad, tal como se explica en el ANEXO III – ¿Qué sabe Google de mí?, más precisamente en el apartado “Lugares en los que estoy y estuve”.
- Un alto porcentaje de encuestados mayores de 65 años, desconocen de qué se trata dichas funcionalidades.

#### Políticas de seguridad de las redes sociales

- Más del 85% de los encuestados, nunca leyó la política de seguridad de las redes sociales que emplea (Gráfico 68). Este número habla a las claras de la relevancia que se le da a la misma. Muy probablemente esto esté relacionado con el pensamiento de aceptarlas independientemente de lo que dichas políticas impliquen. Y es ahí donde las empresas se hacen de la información de sus usuarios, “con su consentimiento”.
- El 3,9% de los encuestados siquiera sabe de qué se trata una política de seguridad (Gráfico 68). Si bien el porcentaje no es del todo significativo, resulta al menos

preocupante el hecho que haya gente que desconozca no el contenido de la política, sino la razón de ser de la misma.

#### Configuración de opciones de privacidad

- Casi el 20% de los encuestados no modificó las opciones de configuración de privacidad. Es decir que su configuración de privacidad está como por defecto. (Gráfico 69). Teniendo en cuenta la masividad del uso de las redes sociales, estos porcentajes corresponden a millones de usuarios que pueden ser presa fácil del robo de información. Para hacer sólo una estimación (ya que se emplean datos de cantidad de usuarios a nivel mundial con porcentajes obtenidos a través de una encuesta regional), sólo teniendo en cuenta Facebook (que tiene 2.414 millones de usuarios en el mundo según Gráfico 20), ese 20% (correspondiente a usuarios que no modificaron las opciones de privacidad), equivaldría a más de 120 millones de usuarios a nivel mundial.
- Entre los encuestados mayores de 65 años, el porcentaje que dice haber personalizado dichas opciones, es de tan sólo el 35,3% (Gráfico 70). El más bajo entre todos los grupos etarios. Es decir que casi el 65% tiene dichas opciones configuradas como por defecto. Esto podría traducirse en un alto nivel de vulnerabilidad en los usuarios contenidos en este rango etario.

#### Contraseñas

- El 12,5% de los encuestados emplean la misma contraseña para todas las aplicaciones que usan (Gráfico 71). Esto es un dato que obviamente los usuarios malintencionados también conocen, y del que en muchos casos sacan provecho para robar información. Este número debería, de manera ideal, tender a cero.
- Sólo el 35% personaliza las contraseñas para cada aplicación (Gráfico 71). Obviamente esta es una práctica más que recomendable a tener en cuenta para proteger la información personal.

#### Robo de información:

- Casi el 55% de los encuestados conoce a alguien que sufrió robo de algún tipo de información (Gráfico 75). Sin embargo, este factor no altera su comportamiento en su relación con las TICs.
- La diferencia entre los encuestados que si conocen a alguien que haya sufrido robo de información, respecto a los que no conocen, se hace más marcada en los rangos etarios

de menor edad. En los cuatro primeros rangos etarios, de hecho la diferencia a favor del “Si” es más notoria que para el resto (Gráfico 76).

#### Uso de redes WiFi

- Más del 84% de los encuestados hace uso de redes WiFi públicas (Gráfico 77), exponiendo su información y sus credenciales a un gran número de posibles ataques tal como se detalla en los artículos de WeLiveSecurity (Riesgos asociados a las redes Wi-Fi públicas - ESET, 2019) y de Infobae (Jaimovich, 2019) .
- Si tomamos que el uso de este tipo de redes está dado por la suma de las opciones 1 (“Siempre que puedo”) y 2 (“De vez en cuando”) (Gráfico 79):
  - o Nivel Primario => 68,8%
  - o Nivel Secundario => 81,7%
  - o Nivel Universitario => 84,4%
  - o Nivel Posgrado => 90,7%

Obtenemos que, inversamente a lo que se podría suponer, a mayor nivel de estudios, mayor el porcentaje de uso de este tipo de redes.

#### Recolección de información por parte de Google.

- El 17,7% de los encuestados dice que no sabía sobre la recolección de información de Google (Gráfico 80).
- El 28,9% de los encuestados dice que no le importa el hecho que Google recolecte información (Gráfico 80). El dato que al 71% restante si le importe, coincide con lo reportado por Amnistía Internacional a través de una encuesta (Amnistía Internacional, 2019), en donde se afirma que *“el 71% de las personas de 9 países siente preocupación por cómo estas empresas recogen y usan sus datos personales”*. Cabe destacar que entre los países citados no se encuentra Argentina, pero está Brasil el cual podría considerarse como comparable. Ese 71%, podría estar interesado en el contenido del presente documento para interiorizarse más al respecto. Se trata de un porcentaje importante de encuestados que serían permeables a una campaña de concientización en la temática abordada.
- Algo similar, pero para usuarios de Estados Unidos, se desprende de la encuesta realizada por Pew Research (Rainie, 218) en donde se afirma que *“Alrededor del 80% de los usuarios de redes sociales dijeron que les preocupaba que los anunciantes y las empresas accedieran a los datos que comparten en las plataformas de redes sociales.”*



Los porcentajes de desconocimiento y de desinterés respecto a la recolección de datos por parte de Google antes citados, se disgregan de la siguiente manera:

Variable	Valor	No saben (%)	No les importa (%)
<b>Edad</b> (Gráfico 81)	Menor de 18 años	36,8	21
	Entre 18 y 24 años inclusive	5,9	35,3
	Entre 25 y 34 años inclusive	12,2	32,7
	Entre 35 y 44 años inclusive	15,2	32
	Entre 45 y 54 años inclusive	19,3	24,2
	Entre 55 y 64 años inclusive	13,6	27,2
	Mayores de 65 años	41,2	17,7
<b>Género</b> (Gráfico 82)	Femenino	25	23,4
	Masculino	6,6	37,4
<b>Estudios</b> (Gráfico 83)	Primario	43,8	31,3
	Secundario	19,6	24,4
	Universitario	15,5	32,4
	Posgrado	13,8	26,1

En color **verde**, los valores más bajo tanto para el caso en el que se mide el desconocimiento, como en el que se mide el desinterés. En color **rojo**, los valores más altos tanto para el caso en el que se mide el desconocimiento, como en el que se mide el desinterés. La intención del cuadro es mostrar las importantes brechas en valores porcentuales entre los valores en verde, y los valores en rojo.

#### Instalación de cámaras en la vía pública

- El porcentaje de encuestados que manifiesta desacuerdo con la instalación de cámaras por sentirse observado, es sólo del 22,8% (Gráfico 84). A priori podría decirse que es un

porcentaje bajo que podría estar asociado con el desconocimiento de los encuestados sobre los riesgos a la privacidad subyacentes.

#### Sobre los encuestados que dicen conocer a alguien que sufrió un episodio de robo de información

- En ninguno de los cruces realizados, se puede determinar que el hecho de conocer a alguien que haya sufrido un episodio de robo de información, repercuta de alguna manera sobre el comportamiento en el uso de TICs.

#### Seguimiento de buenas prácticas (mínimas)

- Sólo el 7,9% del total de los encuestados ha respondido la encuesta de manera tal que podría inferirse el seguimiento de prácticas recomendables mínimas a la hora de interactuar con TICs.
- Si además se busca un mínimo conocimiento de las políticas de privacidad de las redes sociales que emplean, ese número desciende a sólo el 4,4% del total de los encuestados.

#### **Los encuestados ubicados en el rango etario de entre 18 y 24 años inclusive:**

Se ha observado que este grupo etario cuenta con respuestas a varias de las preguntas realizadas, que se destacan entre el resto, por lo cual se profundiza el análisis haciendo foco en este grupo etario:

- Son los que en más alto porcentaje, publican información sensible en las redes sociales (Gráfico 61).
- Es el único rango etario, en el cual los encuestados que se arrepintieron de algo publicado, supera y ampliamente, el porcentaje de los que nunca tuvieron la experiencia de arrepentirse de algo publicado (Gráfico 65).
- Son los que en mayor medida utilizan las funcionalidades de geolocalización en sus dispositivos móviles, siempre que una aplicación se lo solicita (Gráfico 66).

Esto coincide con lo publicado en (Segran, 2014) donde se afirma que los millennials (nacidos entre 1982 y 1994) *“son los que en mayor proporción están dispuestos a compartir su ubicación con las empresas para recibir algún tipo de beneficios con las empresas cercanas.”*

- Junto con los encuestados de entre 55 y 64 años, son los únicos grupos etarios en los que ninguno de los encuestados dice desconocer las opciones de privacidad de los perfiles de sus redes sociales (Gráfico 70).

- Son los que tienen el menor porcentaje de encuestados que emplean contraseñas distintas para cada aplicación (Gráfico 72). A su vez, después de los menores de 18 años, son los que en mayor porcentaje respondieron tener la misma contraseña para todo o casi todo (Gráfico 72).
- Son los que con el porcentaje más alto respondió conocer gente que sufrió robo de información (Gráfico 76).
- Con notable diferencia, son los que más usan las redes WiFi gratuitas. A su vez, son los que más respondieron que las usan “Siempre que pueden” (Gráfico 78).
- Son los que en menor proporción, manifiestan no saber que Google recolecta información (Gráfico 81). Es decir, que manifiestan más saber del tema.
- Son los que en mayor proporción respondieron que no les importa la recolección de datos personales por parte de Google (Gráfico 81). Es decir, son los más desinteresados en el tema.

Ya se dieron sobradas pruebas dentro del presente documento sobre la recolección de información de los usuarios de TICs por parte de las redes sociales y de otras herramientas como por ejemplo las ofrecidas por Google. En el caso de Argentina los usuarios se vuelcan de manera masiva a las redes sociales, y su uso supera en muchos casos, al promedio de uso en el resto del mundo. A su vez, nuestro país posee una enorme cantidad de usuarios ubicados en el rango de edad considerado como “elegible” para transmitir publicidad, mensajes u otro tipo de contenido a través de este medio. Esta combinación de factores, convierten a los usuarios de TICs de nuestro país (y por consiguiente a los de nuestra ciudad) en un foco apetecible para el accionar no sólo de gigantes tecnológicos como podrían ser Google o Facebook, sino además de cualquier persona (ya sea de manera manual o a través de procesos automatizados) que desee hacerse de su valiosa información.

El cruce entre las respuestas a las distintas preguntas, permite concluir que de alguna u otra manera, los usuarios encuestados mantienen una conducta frente al uso de TICs que lleva a una alta exposición de su información. Si no es por un factor, es por otro. Pero lo cierto es que lo observado se traduce en facilidad para la sustracción de información.

Como se observa a partir de los datos obtenidos a partir de la encuesta, los puntos débiles en la interacción con la tecnología son muchos. Por lo cual se vuelve imperioso en nuestro país, no sólo avanzar con el dictamen de las regulaciones correspondientes que pongan un manto de protección (al menos desde el punto de vista legal) sobre los internautas argentinos, sino además de campañas fuertes de concientización que permitan aumentar el conocimiento en la

temática. El conocer los riesgos, sin duda es el primer paso que nuestra sociedad debe dar para minimizar el impacto de los daños.

Como para hacer una breve síntesis de lo expuesto a lo largo del presente documento de investigación, se ha presentado un escenario en el que se combinan una serie de hechos. A decir:

- Falta de precauciones por parte de los usuarios a la hora de usar las TICs.
- Creciente demanda de información asociada a la temática por parte de los usuarios, y creciente disponibilidad de la misma por parte de los medios.
- Nuevas legislaciones proteccionistas para con el usuario.
- Gran cantidad de riesgos para las empresas que no hagan un esfuerzo en pos de proteger la información que manipulan.
- Diversos beneficios para las empresas que si hagan el esfuerzo de proteger debidamente la información que manipulan.

Esta combinación de factores, ponen del lado de las empresas y de los negocios una gran responsabilidad: “El tratamiento de la información”. La misma ya no debería ser un aspecto menor dejado a consideración por parte de las cúpulas de las mismas. Debería ser un tema excluyente y obligatorio en una nueva “era de la información” en la que el hecho de minimizar su alcance o su impacto, podría tumbar a una empresa o negocio (incluso uno exitoso) en cuestión de minutos a partir de un incidente incluso menor. Y estamos hablando de incidentes comunes, cada vez más frecuentes, y realizados por personas malintencionadas dispersas en todo el mundo que incluso desconocen la empresa que atacan, simplemente la encontraron por internet. No de ataques aislados y poco frecuentes efectuados por empleados despechados.

Desde mi humilde punto de vista, la temática aquí tratada debería ser abordada con mucha más seriedad en el mundo de los negocios. Y por qué no, podría ser un tópico a tratar en el dictado de maestrías orientadas al mundo de los negocios (de las características de este MBA por ejemplo). Sin embargo, poco se discute sobre los riesgos asociados al tratamiento (o mejor dicho al no tratamiento) de la información (que cada vez es más cantidad, y más crítica) manipulada en el mundo de los negocios.

La “información es poder”, por eso su cuidado y protección debe ser un aspecto a tener en cuenta (idealmente) desde el nacimiento mismo de cualquier emprendimiento de negocio. Razones, considero ya se dieron varias...

## ANEXO I – Un mundo cada vez más digital

Tal como se introdujera en el CAPÍTULO III, estamos inmersos en un mundo cada vez más digital. Las relaciones interpersonales, se ven cada vez más afectadas por la inclusión tecnológica, y como ya se comentara con anterioridad, el cambio no piensa detenerse. El presente anexo, introduce algunas estadísticas de relevancia sobre esta penetración digital que el mundo está viviendo. La información aquí contenida, complementa lo expuesto en el CAPÍTULO III del presente documento, y la misma forma parte del reporte trimestral correspondiente al tercer trimestre elaborado en el mes de julio de 2019 por Hootsuite y WeAreSocial (Global Digital - Julio 2019, 2019), del mismo reporte pero elaborado en enero de 2019 (Global Digital - Enero 2019, 2019), y del elaborado en octubre de 2019 (Global Digital - Octubre 2019, 2019).

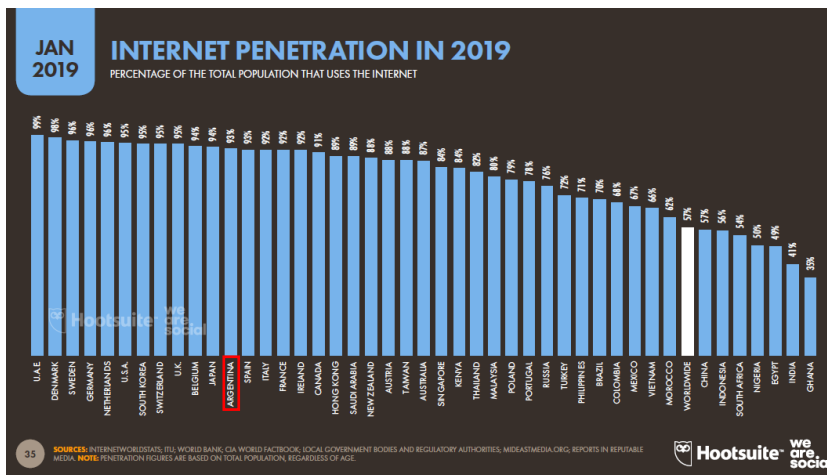


Gráfico 86: Penetración de internet en 2019. Porcentaje dentro del total de la población que usa internet. En nuestro país dicho porcentaje es del

93%, mientras que el promedio mundial es del 57%.

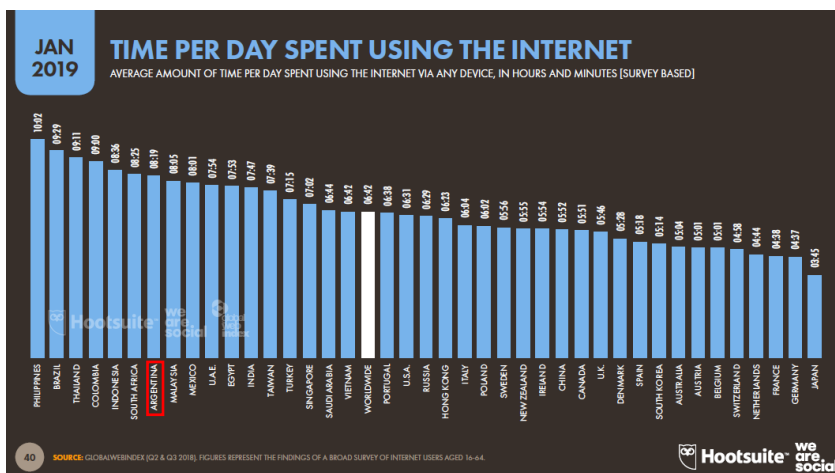


Gráfico 87: Tiempo que cada persona pasa por día usando Internet (vía cualquier dispositivo). Argentina se encuentra por encima del

promedio mundial en cuanto al tiempo empleado en internet (independientemente del

dispositivo empleado). El tiempo promedio en Argentina es de 8 horas 19 minutos y puede verse el detalle desglosado en el Gráfico 11.

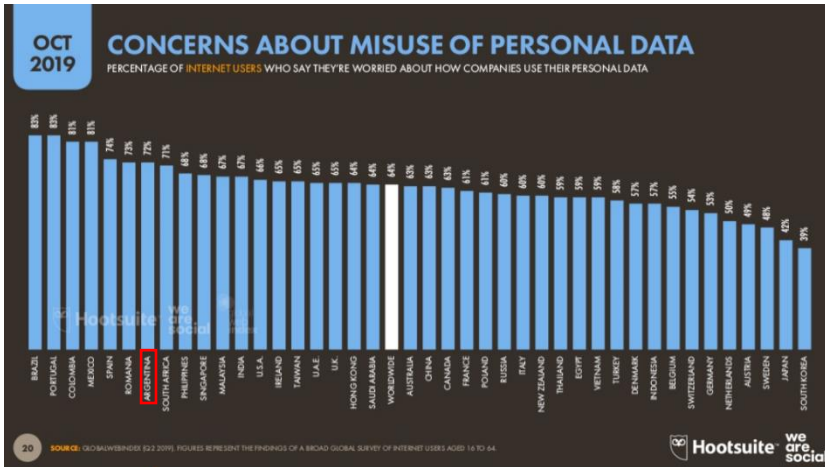


Gráfico 88: Preocupación sobre el mal uso de los datos personales. Este cuadro muestra cuánto **dicen** los internautas de cada país que les preocupa la manera en que las

compañías emplean sus datos personales. Según el mismo, Argentina (72%) se encuentra 8 puntos porcentuales por encima del promedio mundial (64%). Esto no necesariamente tiene relación con las acciones que luego realizan en pos de maximizar su privacidad, pero es, a priori, un buen indicador.

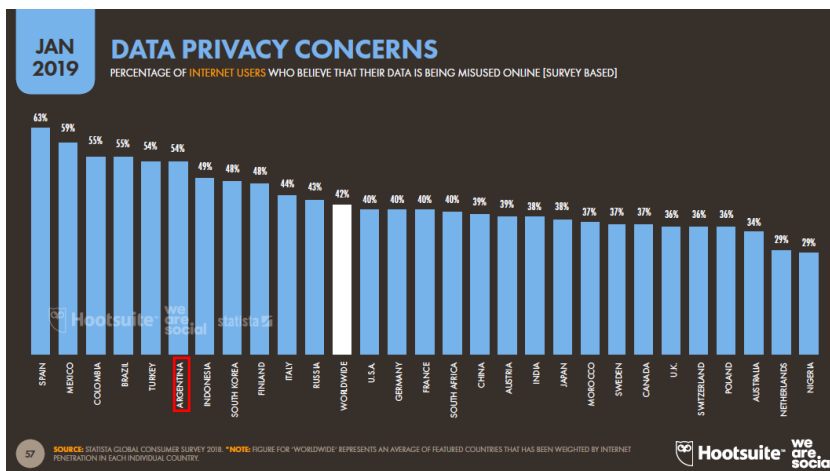


Gráfico 89: Preocupación sobre la privacidad de los datos. Este cuadro muestra el porcentaje de usuarios que creen que sus datos son

mal utilizados. Según el mismo, Argentina se encuentra 12 puntos porcentuales por encima del promedio mundial. Al igual que lo ilustrado mediante el Gráfico 88, esto no necesariamente tiene relación con las acciones que luego realizan en pos de maximizar su privacidad, pero es, a priori, un buen indicador.



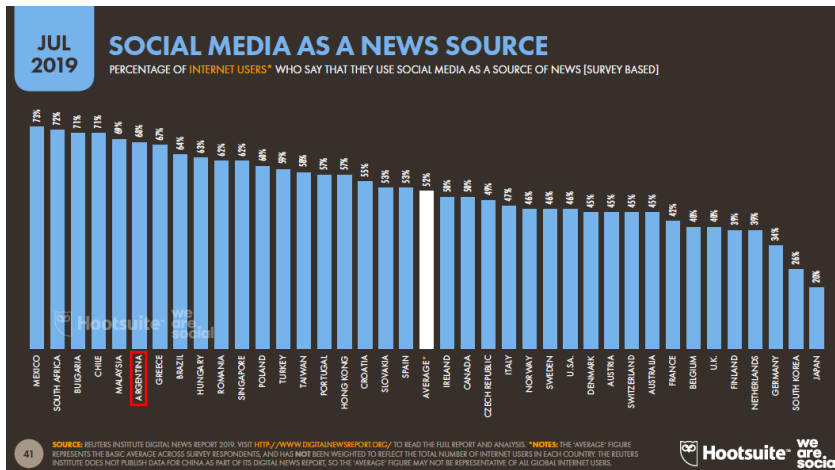


Gráfico 92: Uso de redes sociales como origen de noticias. Porcentaje de usuarios de internet que dicen emplear las redes sociales, como

medio para informarse. Argentina se encuentra con un 68%, muy por encima del promedio mundial (52%).

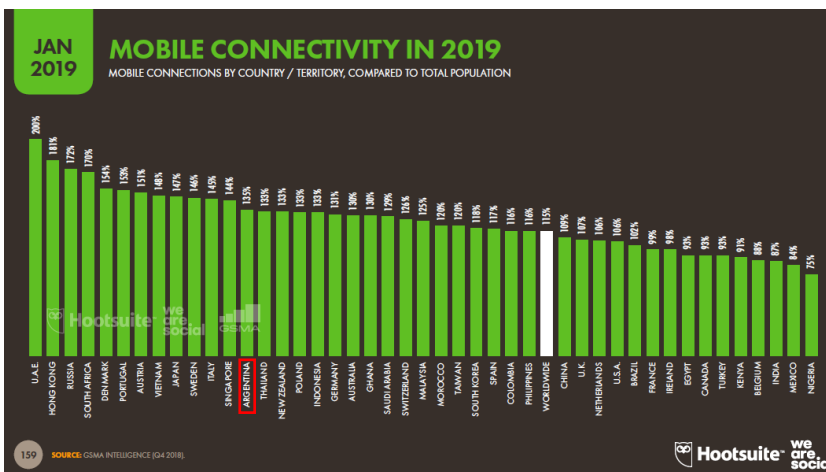


Gráfico 93: Conectividad móvil en 2019. Conexiones móviles comparado con la población total por país o territorio. En nuestro país, la relación entre

cantidad de suscripciones y población, es de 135%. El promedio mundial es de 115%. En ambos casos la cantidad de suscripciones supera la cantidad de pobladores.

### La explosión de las Redes sociales

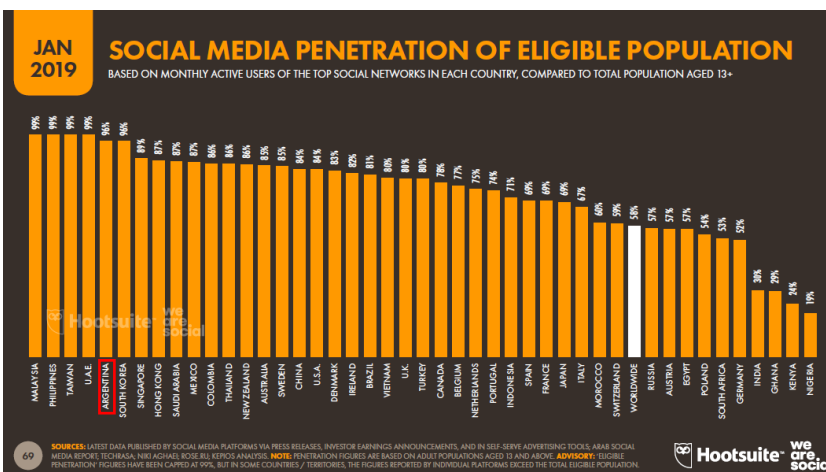


Gráfico 94: Penetración de las redes sociales de población elegible. Basado en usuarios activos de las redes sociales más empleadas en cada país comparado con



los totales poblacionales de mayores de 13 años. Podemos encontrar a nuestro país entre los países con mayor penetración, con un 96%, muy por encima del 58% del promedio mundial.

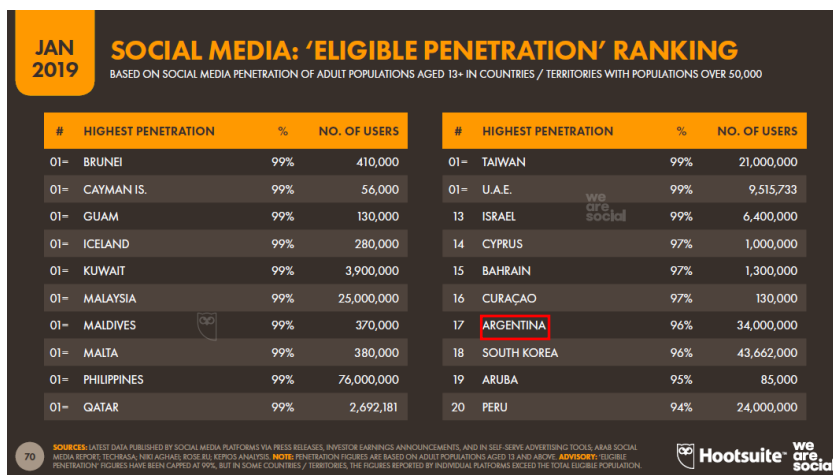


Gráfico 95: Redes sociales: Ranking de “penetración elegible”. Basado en usuarios activos de las redes sociales mayores a 13 años (población elegible), en

países/territorios con población mayor a 50.000 personas. Nótese que Argentina se encuentra posicionado en el lugar 17 dentro de este ranking mundial, pero con un gran número de usuarios (34 millones), sólo superado por Filipinas entre los países que lo preceden.

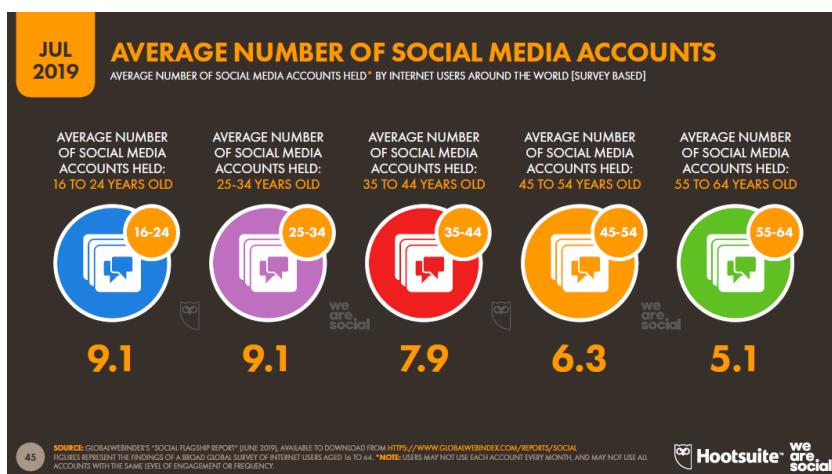


Gráfico 96: Promedio de cantidad de cuentas en redes sociales. Promedio de cantidad de cuentas en redes sociales por cada

usuario de internet en el mundo. Divide los promedios en rangos etarios.

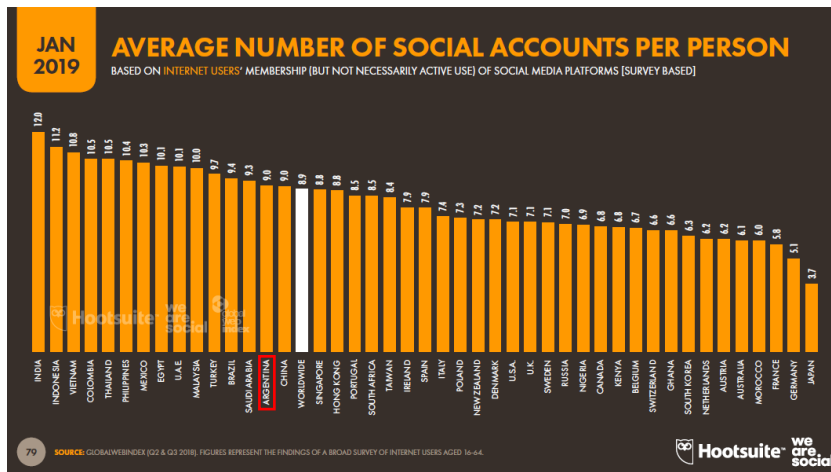


Gráfico 97: Promedio de cantidad de cuentas en redes sociales por persona. Medido en el mundo. No necesariamente

usuarios activos. En Argentina, el promedio es de 9 cuentas de redes sociales por usuario de internet.

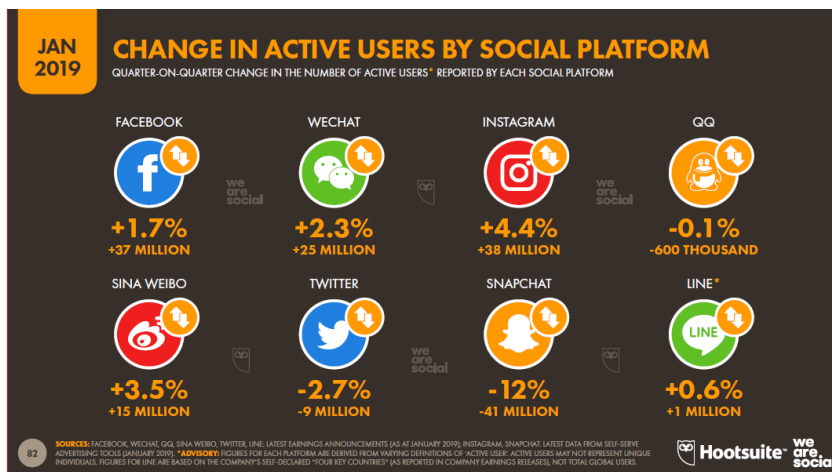


Gráfico 98: Variación en la cantidad de usuarios activos por plataforma social.

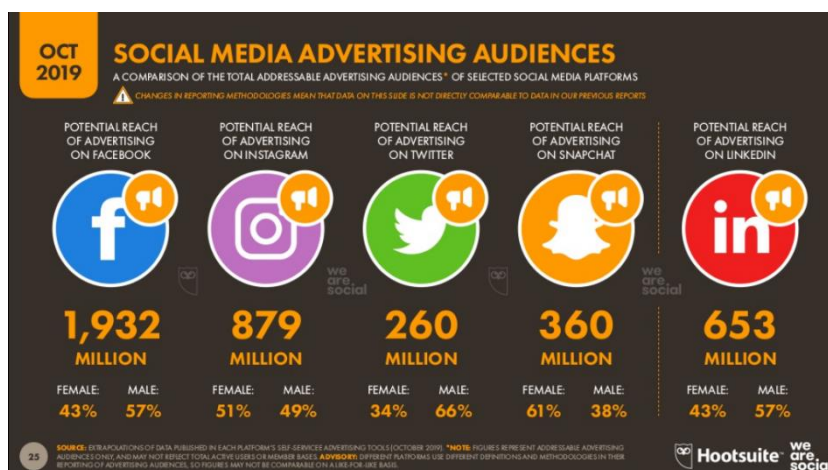


Gráfico 99: Audiencia sobre la cual se podría publicitar en redes sociales. Comparación de la totalidad de la audiencia sobre la cual se podría

publicitar en redes sociales seleccionadas.



Gráfico 100:  
 Ranking de países con las más grandes audiencias para publicitar a través de Facebook. Lista de países ordenados por cantidad de

personas sobre las que se podría publicitar empleando la red social Facebook. A su vez, de esa cantidad proporciona el porcentaje de personas mayores a 13 años (población elegible).

Argentina se encuentra en la posición 17 dentro de dicho ranking, con 29 millones de usuarios a los que se podría llegar, de los cuales el 82% se trata de mayores de 13 años.

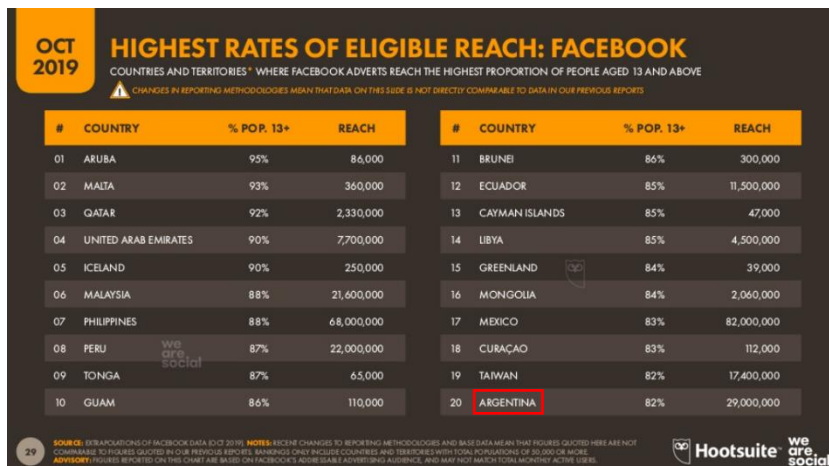


Gráfico 101:  
 Ranking de porcentajes de alcance elegible en Facebook. Países y territorios en donde Facebook llega a través de la

publicidad a más gente mayor de 13 años (público elegible). Argentina se posiciona en el lugar 20, con un total de 29 millones de usuarios de los cuales el 82% corresponde a mayores de 13 años.

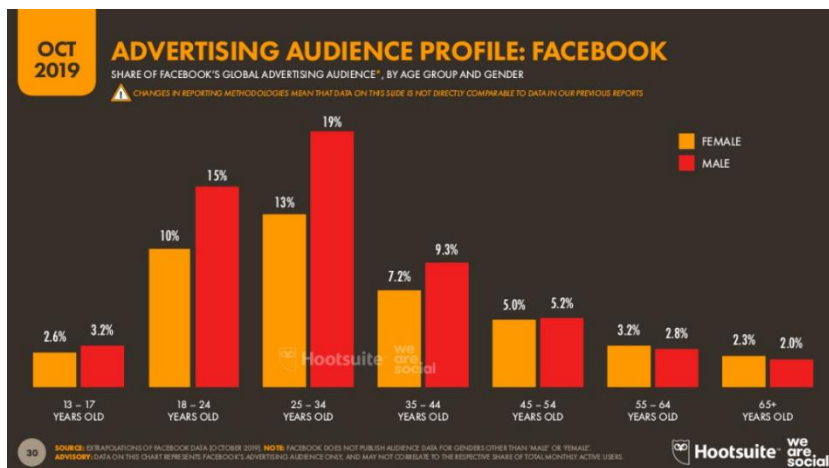


Gráfico 102: Perfil de la audiencia para publicitar a través de Facebook. Porcentaje de cada perfil, tipificado por rango etario, y género.

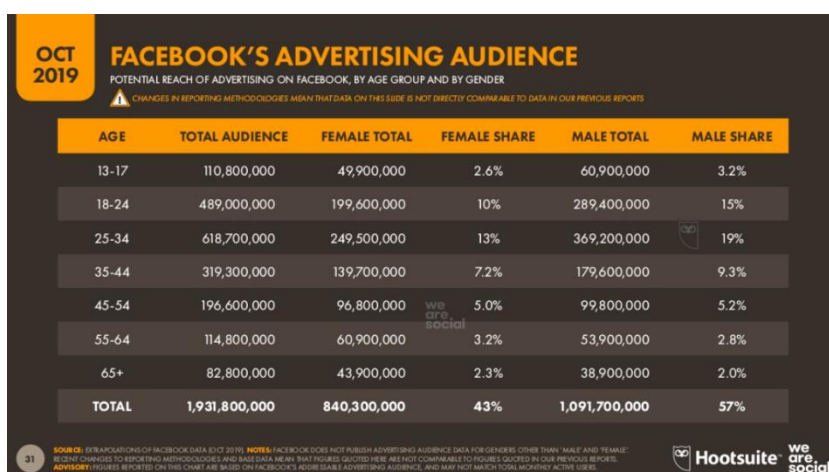


Gráfico 103: Audiencia para publicitar con Facebook. Totales de cada tipo de perfil, tipificado por rango etario, y género.

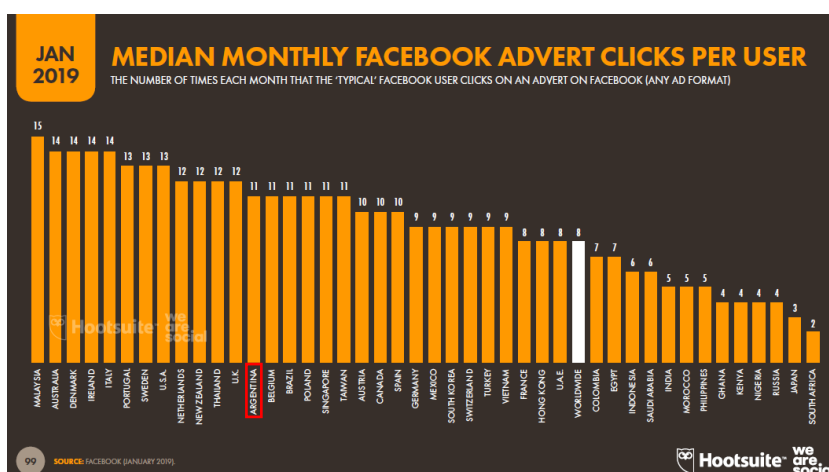


Gráfico 104: Media mensual de clics por usuario en anuncios de Facebook. Cantidad de veces al mes que un usuario "típico" de Facebook hace clic en un anuncio de cualquier

formato. Podemos encontrar a Argentina con 11 clics por usuario por mes, cerca de los países con máxima cantidad de clics por usuario en anuncios (15). Mientras el promedio mundial es de 8 clics. Recordemos que el modelo de negocio de Facebook está basado, en parte, en la venta de publicidad.

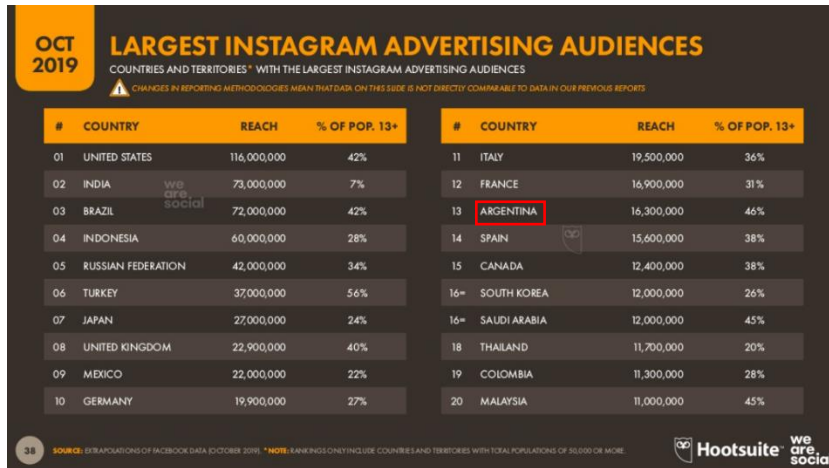


Gráfico 105:  
Ranking de países con las más grandes audiencias para publicitar a través de Instagram. Lista de países ordenados por cantidad de

personas sobre las que se podría publicitar empleando la red social Instagram. A su vez, de esa cantidad proporciona el porcentaje de personas mayores a 13 años (población elegible).

Argentina se encuentra en la posición 13 dentro de dicho ranking, con 16,3 millones de usuarios a los que se podría llegar, de los cuales el 46% se trata de mayores de 13 años. Nuestro país se encuentra entre los países con mayor cantidad de audiencia, en Instagram.

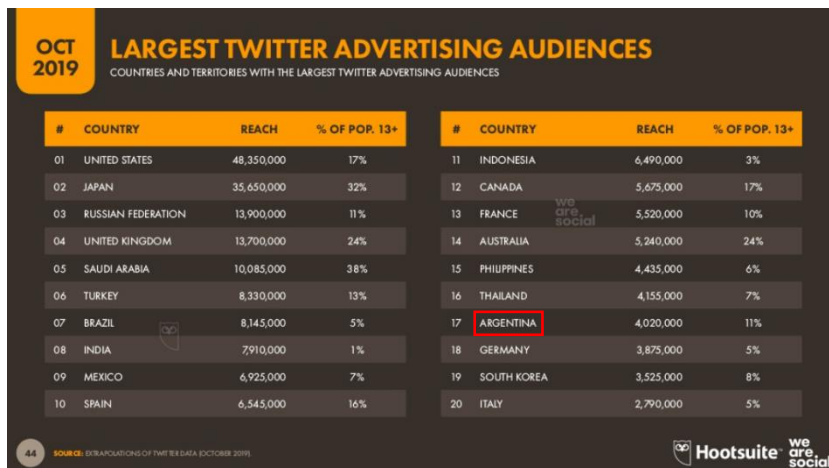


Gráfico 106:  
Ranking de países con las más grandes audiencias para publicitar a través de Twitter. Lista de países ordenados por cantidad de

personas sobre las que se podría publicitar empleando la red social Twitter. A su vez, de esa cantidad proporciona el porcentaje de personas mayores a 13 años (población elegible).

Argentina se encuentra en la posición 17 dentro de dicho ranking, con más de 4 millones de usuarios a los que se podría llegar, de los cuales el 11% se trata de mayores de 13 años. Nuestro país se encuentra entre los países con mayor cantidad de audiencia, en Twitter.

## ANEXO II – Condiciones de servicio de Facebook

### **Política de Datos** (Facebook - Política de Datos, 2018)

Se encuentra estructurada de la siguiente manera (las viñetas y la ordenación numérica subordinada no son tal cual las existentes en la política, pero se introducen en el presente documento para hacer más ordenado el análisis):

#### **1. ¿Qué tipo de información recopilamos?**

- 1.1. Lo que tú y otras personas hacen y proporcionan
  - 1.1.1. Información y contenido que nos proporcionas
  - 1.1.2. Datos con protecciones especiales
  - 1.1.3. Redes y conexiones
  - 1.1.4. Tu uso
  - 1.1.5. Información sobre transacciones realizadas en nuestros Productos.
  - 1.1.6. La actividad de otros usuarios y la información que proporcionan sobre ti.
- 1.2. Información de los dispositivos
  - 1.2.1. Atributos del dispositivo
  - 1.2.2. Operaciones del dispositivo
  - 1.2.3. Identificadores
  - 1.2.4. Señales del dispositivo
  - 1.2.5. Datos de la configuración del dispositivo
  - 1.2.6. Red y conexiones
  - 1.2.7. Datos de cookies
- 1.3. Información de los socios

#### **2. ¿Cómo usamos esta información?**

- 2.1. Proporcionamos, personalizamos y mejoramos nuestros Productos.
  - 2.1.1. Información de los dispositivos y Productos de Facebook
  - 2.1.2. Información relacionada con la ubicación
  - 2.1.3. Investigación y desarrollo de productos:
  - 2.1.4. Reconocimiento facial
  - 2.1.5. Anuncios y otro contenido publicitario
- 2.2. Ofrecemos mediciones, análisis y otros servicios empresariales
- 2.3. Fomentamos la seguridad, la integridad y la protección.
- 2.4. Nos comunicamos contigo.

2.5. Realizamos investigaciones e innovamos en pro del bienestar social.

### 3. ¿Cómo se comparte esta información?

#### 3.1. En Productos de Facebook

3.1.1. Personas y cuentas con las que te comunicas y compartes información

3.1.2. Contenido que otros comparten o vuelven a compartir acerca de ti

3.1.3. Información sobre tu estado activo o presencia en nuestros Productos

3.1.4. Aplicaciones, sitios web e integraciones de terceros en nuestros Productos o que usan nuestros Productos.

3.1.5. Propietario nuevo

#### 3.2. Con socios externos

3.2.1. Socios que usan nuestros servicios de análisis.

3.2.2. Anunciantes

3.2.3. Socios de medición

3.2.4. Socios que ofrecen bienes y servicios en nuestros Productos.

3.2.5. Vendedores y proveedores de servicios.

3.2.6. Investigadores y académicos.

3.2.7. Autoridades y solicitudes legales.

## 1. ¿QUÉ TIPO DE INFORMACIÓN RECOPILAMOS?

### 1.1. Lo que tú y otras personas hacen y proporcionan:

1.1.1. Información y contenido que nos proporcionas .... información en el contenido, o sobre él, que proporcionas (como los metadatos), por ejemplo, la ubicación de una foto o la fecha de creación de un archivo. También puede incluir el contenido que ves a través de las funciones que proporcionamos, como la cámara...

1.1.2. Datos con protecciones especiales: puedes optar por proporcionar información en los campos de tu perfil de Facebook o acontecimientos importantes relacionados con tus creencias religiosas, tus ideologías políticas, tus intereses o aspectos relacionados con tu salud. Esta y otra información (como el origen étnico o racial, las creencias filosóficas o la afiliación sindical) puede estar sujeta a protecciones especiales en virtud de las leyes de tu país.

1.1.3. Redes y conexiones: Recopilamos información sobre las personas, las páginas, las cuentas, los hashtags y los grupos a los que estás conectado y cómo interactúas

*con ellos a través de nuestros Productos, como las personas con las que más te comunicas o los grupos de los que formas parte. También recopilamos información de contacto si eliges subirla, sincronizarla o importarla desde un dispositivo (como una libreta de direcciones, un registro de llamadas o un historial de SMS) ...*

*1.1.4. Tu uso: Recopilamos información sobre cómo usas nuestros Productos, como los tipos de contenido que ves o con los que interactúas, las funciones que utilizas, las acciones que llevas a cabo, las personas o cuentas con las que interactúas, y la hora, la frecuencia y la duración de tus actividades. Por ejemplo, registramos cuándo estás usando y cuándo usaste por última vez nuestros Productos, y qué publicaciones, videos y otro tipo de contenido ves en nuestros Productos. También recopilamos información sobre cómo usas funciones como nuestra cámara.*

*1.1.5. Información sobre transacciones realizadas en nuestros Productos: Si usas nuestros Productos para efectuar compras u otras transacciones financieras (por ejemplo, cuando realizas una compra en un juego o haces una donación), recopilamos información sobre dicha compra o transacción. Esto incluye información de pago, como el número de tu tarjeta de crédito o débito y otra información sobre la tarjeta; otra información sobre la cuenta y la autenticación; y detalles de facturación, envío y contacto.*

*1.1.6. La actividad de otros usuarios y la información que proporcionan sobre ti: También recibimos y analizamos contenido, comunicaciones e información que nos proporcionan otras personas al usar nuestros Productos. Esto puede incluir información sobre ti, como en el caso de que otras personas compartan o comenten una foto tuya, te envíen un mensaje o suban, sincronicen o importen tu información de contacto.*

## **1.2. Información de los dispositivos**

*.. recopilamos información de las computadoras, los teléfonos, los televisores conectados y otros dispositivos conectados a la web que usas y que se integran con nuestros Productos, y combinamos esta información entre los diferentes dispositivos que empleas. Por ejemplo, usamos la información que recopilamos sobre cómo usas nuestros Productos en tu teléfono para personalizar mejor el contenido (incluidos los anuncios) o las funciones que ves cuando usas nuestros Productos en otro dispositivo, como tu computadora portátil o tableta, o para*



*medir si realizaste una acción en respuesta a un anuncio que te mostramos en tu teléfono o en otro dispositivo.*

*La información que obtenemos de estos dispositivos incluye:*

*1.2.1. Atributos del dispositivo: información como el sistema operativo, las versiones de hardware y software, el nivel de carga de la batería, la potencia de la señal, el espacio de almacenamiento disponible, el tipo de navegador, los tipos y nombres de aplicaciones y archivos, y los plugins.*

*1.2.2. Operaciones del dispositivo: información sobre las operaciones y los comportamientos realizados en el dispositivo, como poner una ventana en primer o segundo plano, o los movimientos del mouse (lo que permite distinguir a humanos de bots).*

*1.2.3. Identificadores: identificadores únicos, identificadores de dispositivos e identificadores de otro tipo, como aquellos provenientes de juegos, aplicaciones o cuentas que usas, así como identificadores de dispositivos familiares (u otros identificadores exclusivos de los Productos de las empresas de Facebook y que se vinculan con la misma cuenta o el mismo dispositivo).*

*1.2.4. Señales del dispositivo: señales de Bluetooth e información sobre puntos de acceso a wifi, balizas (“beacons”) y torres de telefonía celular cercanos.*

*1.2.5. Datos de la configuración del dispositivo: información que nos permites recibir mediante la configuración que activas en tu dispositivo, como el acceso a la ubicación de GPS, la cámara o las fotos.*

*1.2.6. Red y conexiones: información, como el nombre del operador de telefonía celular o proveedor de internet, el idioma, la zona horaria, el número de teléfono celular, la dirección IP, la velocidad de la conexión y, en algunos casos, información sobre otros dispositivos que se encuentran cerca o están en tu red, para que podamos hacer cosas como ayudarte, por ejemplo, a transmitir un video del teléfono al televisor.*

*1.2.7. Datos de cookies: datos provenientes de las cookies almacenadas en tu dispositivo, incluidos la configuración y los identificadores de cookies...*

### **1.3. Información de los socios.**

*Los anunciantes, los desarrolladores de aplicaciones y los editores pueden enviarnos información por medio de las herramientas empresariales de Facebook que usan, incluidos nuestros plugins sociales (como el botón “Me gusta”), el inicio de sesión con Facebook, nuestras API y SDK, o el píxel de Facebook. Estos socios nos brindan información sobre las actividades que realizas fuera de Facebook, incluidos datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que haces, los anuncios que ves y la manera en la que usas sus servicios, ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella. Por ejemplo, un desarrollador de juegos podría usar nuestra API para contarnos en qué juegos participas, o bien un negocio podría informarnos sobre la compra que hiciste en su tienda. Asimismo, también recibimos información sobre las acciones y las compras que realizas dentro y fuera de internet por parte de proveedores de datos externos que están autorizados a proporcionarnos tu información.*

*Los socios reciben tus datos cuando visitas o usas sus servicios, o a través de socios externos con los que trabajan. Para que nos puedan facilitar cualquier tipo de información, exigimos que todos los terceros cuenten con derechos legítimos para recopilar, usar y compartir tus datos.*

## **2. ¿CÓMO USAMOS ESTA INFORMACIÓN?**

### **2.1. Proporcionamos, personalizamos y mejoramos nuestros Productos:**

*... para personalizar las funciones y el contenido (incluidos la sección de noticias, el feed de Instagram, Instagram Stories y los anuncios) y hacerte sugerencias (como grupos o eventos que pueden interesarte o temas que quizás quieras seguir) tanto dentro como fuera de nuestros Productos. Con el objetivo de crear Productos personalizados que sean únicos y relevantes para ti, usamos tus conexiones, preferencias, intereses y actividades en función de los datos que recopilamos y que tú y otras personas nos proporcionan (incluidos aquellos datos con protecciones especiales que decides facilitarnos), así como la forma en la que usas nuestros Productos e interactúas con ellos, y las personas, los lugares o las cosas con los que te conectas y que te interesan, tanto dentro como fuera de nuestros Productos.*

*2.1.1. Información de los dispositivos y Productos de Facebook: vinculamos la información sobre tus actividades en diferentes dispositivos y Productos de Facebook*

*para proporcionar una experiencia más personalizada y uniforme en todos ellos, donde sea que los uses. Por ejemplo, podemos sugerir que te unas a un grupo en Facebook que incluye a personas que sigues en Instagram o con las que te comuniques por medio de Messenger. También podemos optimizar tu experiencia, por ejemplo, completando automáticamente tu información de registro (como tu número de teléfono) de un Producto de Facebook cuando te registres para abrir una cuenta en otro Producto.*

*2.1.2. Información relacionada con la ubicación: usamos la información relacionada con la ubicación, como tu ubicación actual, el lugar donde vives y los lugares que te gusta visitar, así como las empresas y las personas que se encuentran cerca de ti, para proporcionar, personalizar y mejorar nuestros Productos, incluidos los anuncios, a fin de que resulten más relevantes para ti y otras personas. La información relacionada con la ubicación puede basarse en factores como la ubicación exacta del dispositivo (si nos permitiste recopilar esta información), direcciones IP e información sobre el uso que tú y otras personas hacen de los Productos de Facebook (como visitas registradas y eventos a los que asistes).*

*2.1.3. Investigación y desarrollo de productos: usamos la información que tenemos para desarrollar, probar y mejorar nuestros Productos, incluido por medio de encuestas e investigaciones, y para pruebas y solución de problemas de funciones y productos nuevos.*

*2.1.4. Reconocimiento facial: si se activa esta función, usaremos la tecnología de reconocimiento facial para reconocerte en fotos, videos y experiencias de la cámara. Las plantillas de reconocimiento facial que creamos pueden constituir datos con protecciones especiales en virtud de la legislación de tu país...*

*2.1.5. Anuncios y otro contenido publicitario: usamos la información que tenemos sobre ti, incluida información sobre tus intereses, acciones y conexiones, para seleccionar y personalizar anuncios, ofertas y otro contenido publicitario que te mostramos.*

## **2.2. Ofrecemos mediciones, análisis y otros servicios empresariales.**

*Usamos la información que tenemos (incluida la actividad que realizas fuera de nuestros Productos, como los sitios web que visitas y los anuncios que ves) para ayudar a los anunciantes y otros socios a medir la eficacia y la distribución de sus anuncios y servicios, así*

*como para ayudarlos conocer qué tipos de personas usan sus servicios y cómo interactúan con sus sitios web, aplicaciones y servicios.*

### **2.3. Fomentamos la seguridad, la integridad y la protección.**

*Usamos la información que tenemos para verificar cuentas y actividades, combatir conductas perjudiciales, detectar y prevenir spam y otras experiencias negativas...*

### **2.4. Nos comunicamos contigo.**

*Usamos la información que tenemos para enviarte mensajes de marketing, comunicarnos contigo sobre nuestros Productos e informarte acerca de nuestras políticas y condiciones...*

### **2.5. Realizamos investigaciones e innovamos en pro del bienestar social.**

*Utilizamos la información que tenemos (incluida aquella proveniente de los socios de investigación con los que trabajamos) para llevar a cabo y respaldar investigaciones e innovaciones relacionadas con el bienestar social general, los avances tecnológicos, y el interés, la salud y el bienestar públicos. Por ejemplo, analizamos la información que tenemos sobre los patrones migratorios durante una situación de emergencia para respaldar las iniciativas de ayuda humanitaria.*

## **3. ¿CÓMO SE COMPARTE ESA INFORMACIÓN?**

*Tu información se comparte con otros de las siguientes formas:*

### **3.1 En Productos de Facebook**

*3.1.1 Personas y cuentas con las que te comunicas y compartes información: Cuando te comunicas y compartes información usando nuestros Productos, eliges el público que puede ver lo que compartes. Por ejemplo, cuando publicas algo en Facebook, seleccionas el público al que va dirigida la publicación, que puede ser un grupo, todos tus amigos, el público general o una lista personalizada de gente. De un modo similar, cuando usas Messenger o Instagram para comunicarte con personas o negocios, estos últimos pueden ver el contenido que envías. Los miembros de tu red también pueden*

*ver las acciones que realizaste en nuestros Productos, como la interacción que mantuviste con los anuncios y el contenido patrocinado. También permitimos que otras cuentas vean quién vio sus historias de Facebook o Instagram. Cualquier persona puede ver la información pública, tanto dentro como fuera de nuestros Productos, aunque no tenga una cuenta. Esto incluye tu nombre de usuario de Instagram, la información que compartes con el público, información de tu perfil público en Facebook y contenido que compartes en una página de Facebook, una cuenta pública de Instagram o cualquier foro de carácter público, como Facebook Marketplace. Tú, otras personas que usan Facebook e Instagram y nosotros podemos conceder acceso a información pública o enviar dicha información a cualquier persona, tanto dentro como fuera de nuestros Productos, incluido en otros Productos de las empresas de Facebook, en resultados de búsqueda o por medio de herramientas y API...*

*3.1.2. Contenido que otros comparten o vuelven a compartir acerca de ti: Te recomendamos que pienses bien con quién quieres compartir contenido, ya que las personas que ven tu actividad en nuestros Productos pueden decidir compartirla con otras tanto dentro como fuera de ellos, incluidos negocios y personas que no pertenecen al público que elegiste. Por ejemplo, si compartes una publicación o envías un mensaje a un amigo o a una cuenta determinados, estos pueden tomar una captura de pantalla de dicho contenido o bien descargarlo o volver a compartirlo con otras personas dentro o fuera de nuestros Productos, en persona o en experiencias de realidad virtual, como Facebook Spaces. Asimismo, cuando comentas la publicación de otra persona o reaccionas a su contenido, cualquiera que pueda ver el contenido de esa persona verá también el comentario o la reacción, y esa persona puede cambiar su público más adelante.*

*Las personas también pueden usar nuestros Productos para crear y compartir contenido sobre ti con el público que elijan. Por ejemplo, pueden compartir una foto tuya en una historia, mencionarte o etiquetarte en una ubicación determinada en una publicación, o bien compartir información acerca de ti en sus publicaciones o mensajes.*

*3.1.3. Información sobre tu estado activo o presencia en nuestros Productos: Hay señales que indican a las personas que forman parte de tus redes si estás activo en*

*nuestros Productos, incluido si estás activo en ese momento en Instagram, Messenger o Facebook, o cuándo fue la última vez que usaste nuestros Productos.*

*3.1.4. Aplicaciones, sitios web e integraciones de terceros en nuestros Productos o que usan nuestros Productos: Cuando decides usar aplicaciones, sitios web u otros servicios de terceros que utilizan nuestros Productos o están integrados con ellos, estas plataformas pueden recibir información acerca de tus publicaciones o del contenido que compartes. Por ejemplo, cuando juegas a un juego con tus amigos de Facebook o usas los botones “Comentar” o “Compartir” de Facebook en un sitio web, el sitio web o el desarrollador del juego pueden recibir información sobre tus actividades en el juego, o un comentario o enlace de su sitio web que compartas en Facebook. Asimismo, cuando descargas o usas servicios de terceros, estos pueden acceder a tu perfil público de Facebook, así como a cualquier información que compartas con ellos. Los sitios web y las aplicaciones que usas pueden tener acceso tu lista de amigos de Facebook si eliges compartirla con ellos. No obstante, no podrán recibir otro tipo de información sobre tus amigos de Facebook ni sobre tus seguidores de Instagram (aunque, desde luego, estos pueden elegir compartir esa información). La información que recopilan estos servicios de terceros está sujeta a sus propias condiciones y políticas, no al presente documento.*

*Los dispositivos y sistemas operativos que ofrecen versiones nativas de Facebook e Instagram (en los casos en donde no desarrollamos nuestras propias aplicaciones) tendrán acceso a todos los datos que decidas compartir con ellos, incluida la información que tus amigos comparten contigo, para poder ofrecerte nuestra funcionalidad principal.*

*3.1.5. Propietario nuevo: Si cambia la propiedad o el control de la totalidad o de una parte de nuestros Productos o de sus activos, podemos transferir tu información al nuevo propietario.*

### **3.2. Con socios externos**

*Colaboramos con socios externos que nos ayudan a proporcionar y mejorar nuestros Productos, o que usan las Herramientas empresariales de Facebook para hacer crecer sus negocios, lo que hace posible que operemos nuestras empresas y proporcionemos servicios*

*gratuitos a personas de todo el mundo... Estos son los tipos de socios externos con los que compartimos información:*

*3.2.1 Socios que usan nuestros servicios de análisis: Proporcionamos estadísticas y observaciones consolidadas que ayudan a las personas y a los negocios a entender cómo interactúan las personas con sus publicaciones, anuncios, páginas, videos y otro contenido dentro y fuera de los Productos de Facebook. Por ejemplo, los administradores de páginas y los perfiles de empresa de Instagram reciben información sobre el número de personas o cuentas que vieron o comentaron sus publicaciones, o reaccionaron a ellas, así como datos demográficos consolidados y otro tipo de información que los ayuda a entender las interacciones con la página o cuenta.*

*3.2.2 Anunciantes: Ofrecemos a los anunciantes informes sobre qué tipos de personas ven sus anuncios y qué resultados generan. No obstante, a menos que nos des permiso para hacerlo, no compartimos información que te identifique personalmente, como tu nombre o dirección de correo electrónico, datos que se pueden usar para ponerse en contacto contigo o que pueden revelar tu identidad. Por ejemplo, brindamos a los anunciantes datos demográficos generales e información sobre intereses (por ejemplo, que una mujer de entre 25 y 34 años que vive en la Ciudad de México y le interesa la ingeniería de software vio un anuncio) para ayudarlos a conocer mejor al público. También confirmamos qué anuncios de Facebook te llevaron a concretar una compra o realizar una acción con un anunciante.*

*3.2.3 Socios de medición: Compartimos información sobre ti con empresas que la consolidan para ofrecer análisis e informes de medición a nuestros socios.*

*3.2.4 Socios que ofrecen bienes y servicios en nuestros Productos: Si te suscribes a contenido premium o compras algo a alguien que vende en nuestros Productos, el creador del contenido o vendedor pueden recibir tu información pública y otros datos que compartes con ellos, así como la información necesaria para completar la transacción, incluidos detalles de contacto y envío.*

*3.2.5 Vendedores y proveedores de servicios: Proporcionamos información y contenido a vendedores y proveedores de servicios que dan soporte a nuestro negocio, como los que proveen servicios de infraestructura técnica, análisis del uso de nuestros Productos, servicios de atención al cliente, administración de pagos o encuestas.*

*3.2.6 Investigadores y académicos: También brindamos información y contenido a socios investigadores y académicos para que realicen investigaciones que permitan profundizar los conocimientos y la innovación que respalden a nuestro negocio o nuestra misión, y refuercen el descubrimiento y la innovación sobre temas relacionados con el bienestar social general, los avances tecnológicos, y el interés, la salud y el bienestar públicos.*

*3.2.7 Autoridades y solicitudes legales: Compartimos información con autoridades o en respuesta a solicitudes legales...*

Siguiendo con el análisis de las Condiciones de servicio, el próximo punto relevante es el punto 3, titulado “Tus compromisos con Facebook y nuestra comunidad”. Dentro de este punto, hay varias cosas interesantes para transcribir que son de particular interés para este análisis. Nos referiremos al punto 3.3 titulado “Los permisos que nos concedes”.

### **3. Permisos que nos concedes**

*Para proporcionar nuestros servicios, necesitamos que nos concedas determinados permisos:*

- *Permiso para usar contenido que creas y compartes: ... en concreto, cuando compartes, publicas o subes contenido que se encuentra protegido por derechos de propiedad intelectual (como fotos o videos) en nuestros Productos, o en relación con ellos, nos otorgas una licencia internacional, libre de regalías, sublicenciable, transferible y no exclusiva para alojar, usar, distribuir, modificar, publicar, copiar, mostrar o exhibir públicamente y traducir tu contenido, así como para crear trabajos derivados de él (de conformidad con tu configuración de privacidad y de la aplicación). En otras palabras, si compartes una foto en Facebook, nos concedes permiso para almacenarla, copiarla y compartirla con otros (por supuesto, de conformidad con tu configuración), como proveedores de servicios que usan nuestros servicios u otros Productos de Facebook que usas. Esta licencia caduca cuando tu contenido se elimina de nuestros sistemas.*

*Cuando eliminas contenido, los demás usuarios dejan de verlo. Sin embargo, puede seguir existiendo en otras partes de nuestros sistemas donde:*



- *no es posible eliminarlo de forma inmediata debido a limitaciones técnicas...*
- *otros hayan usado tu contenido en virtud de esta licencia y esas personas no lo hayan eliminado (en cuyo caso, esta licencia se seguirá aplicando hasta que el contenido sea eliminado); o*
- *la eliminación inmediata restringiría nuestra capacidad para:*
  - o *investigar o identificar actividades ilegales o infracciones de nuestras Condiciones o Políticas (por ejemplo, para identificar o investigar el uso indebido de nuestros Productos o sistemas);*
  - o *cumplir con una obligación legal, como la preservación de pruebas; o*
  - o *cumplir con una solicitud de una autoridad judicial o administrativa, fuerzas del orden o una agencia gubernamental; en cuyo caso, el contenido se retendrá únicamente durante el tiempo que sea necesario para el fin en cuestión (la duración exacta variará según cada caso).*

*En cada uno de los casos anteriores, esta licencia seguirá vigente hasta que el contenido se haya eliminado por completo*
- *Permiso para usar tu nombre, foto del perfil e información sobre las acciones que realizas con anuncios y contenido patrocinado:* *Nos concedes permiso para usar tu nombre y foto del perfil e información sobre las acciones que realizas en Facebook junto a anuncios, ofertas y otro contenido patrocinado que mostramos en nuestros Productos, o en relación con ellos, sin que recibas compensación de ningún tipo. Por ejemplo, podemos mostrar a tus amigos que te interesa un evento publicado o que te gusta una página creada por una marca que nos paga para mostrar sus anuncios en Facebook. Solo se muestra este tipo de anuncios a las personas que tienen tu permiso para ver las acciones que realizas en Facebook ....*

- Permiso para actualizar el software que usas o descargas: Si descargas o usas nuestro software, nos concedes permiso para descargar e instalar actualizaciones del software, donde corresponda.

## ANEXO III – ¿Qué sabe Google de mí?

A lo largo del documento se mencionó a Google como el gran oráculo de internet, el que todo lo sabe. Además, que el gigante tecnológico sabe mucho de cada uno de sus usuarios, y que para ello se basa en inmensidad de métodos para recolectar y cruzar información que quizás nosotros como usuarios brindamos sin notarlo. Si el lector desea tener una noción de qué es todo eso que Google sabe de uno, este anexo brinda una buena aproximación:

**Quién soy:** Información básica sobre mí tal como nombre completo, fecha de nacimiento, género, país de residencia, número de teléfono móvil, una dirección de correo electrónico alternativa entre otros detalles, están contenidos en mi cuenta de Google.

**Mi apariencia:** De una manera bastante sencilla, Google podría tener una buena noción de mi aspecto físico aplicando reconocimiento facial a las fotos subidas a la herramienta *Google Photos*. De hecho, a través de esta herramienta, el usuario puede etiquetar las personas presentes en una imagen, lo cual permitiría también, individualizar cada una de las personas incluidas en cada una de las imágenes subidas. O sea que cuantas más fotos suba, más información sobre esas fotos incorporará, y más precisión sobre mí tendrá el algoritmo de reconocimiento.

**Mi voz:** Si, Google también puede reconocerla. Recordemos que Google emplea todo lo que está a su alcance para retroalimentar sus algoritmos y armar nuestro perfil con la mayor precisión posible. Android tiene lo que se conoce como *Asistente de Google*, a través del cual se le pueden dar instrucciones de manera hablada. Esos mensajes hablados que recibe, sin lugar a duda serán empleados para guardar los patrones de voz en base a sus características. De hecho, uno puede acceder a través de la url <https://myactivity.google.com/myactivity?hl=en&restrict=vaa> al historial de comandos de voz, o registros de voz realizados (dependiendo de la configuración de cada cuenta). En las opciones de configuración de la cuenta, se notifica a los usuarios sobre lo que se almacena. El Gráfico 107, obtenido de la configuración de cuenta, muestra este detalle:

### Qué contenido se guarda en la Actividad de voz y audio

Google graba tu voz y otros audios, además de algunos segundos anteriores, cuando usas activaciones de audio como las siguientes:

- decir comandos de voz como "Ok Google"
- presionar el ícono del micrófono

El audio se guarda en tu cuenta solo si accediste a ella y habilitaste la Actividad de voz y audio. Los audios se pueden guardar incluso cuando el dispositivo está sin conexión.

**Nota:** No todas las apps pueden guardar audio en tu cuenta.

Gráfico 107: Guardado de actividad de audio y voz de Google.

**Mis creencias religiosas / políticas:** Si alguna vez visité el sitio web de un partido político, o de un candidato, o hice algún comentario (bueno o malo) con algún tipo de incumbencia política, o reproduje un video a través de YouTube con algún tinte político, seguramente Google lo empleó para conocer sobre mis inclinaciones políticas. De igual manera sucedería si en lugar de política fuera algo de incumbencia religiosa. Una búsqueda relacionada a una festividad religiosa, algún video o algo que dé a entender qué religión profeso, algún saludo enviado por correo electrónico o por Hangout en relación a cualquier festividad religiosa (“Feliz Navidad”, “Felices Pascuas”, y se me ocurren varios ejemplos más).

**Mi estado de salud:** Al usar *Google Fit*, estaré brindándole a Google una visión general bastante buena de mi aptitud física, y de mi salud. Desde cuán activo soy, las calorías quemadas por día y por qué no, mis objetivos de condición física. Pero incluso si no uso esta aplicación, probablemente Google sea capaz de armar en base a mis búsquedas una “historia clínica” con mayor o menor grado de detalle. Si busco información sobre una enfermedad, un síntoma, un medicamento, un tratamiento, todo será añadido a mi perfil y empleado para sacar conclusiones.

De hecho Google comercializa también diversos dispositivos de hardware entre los que se encuentran relojes inteligentes, a través de los cuales, y tal como se visualiza en la publicidad de relojes inteligentes o Smart watch del Gráfico 108, los mismos vienen provistos con *Asistente de Google* y *Google Fit* (Dispositivos de Google con Google Fit, 2019). Toda la información recolectada por el reloj con *Google Fit*, será luego sincronizada a la cuenta de Google, desde la cual luego podrá ser visualizada desde cualquier otro dispositivo que tenga sincronizado.

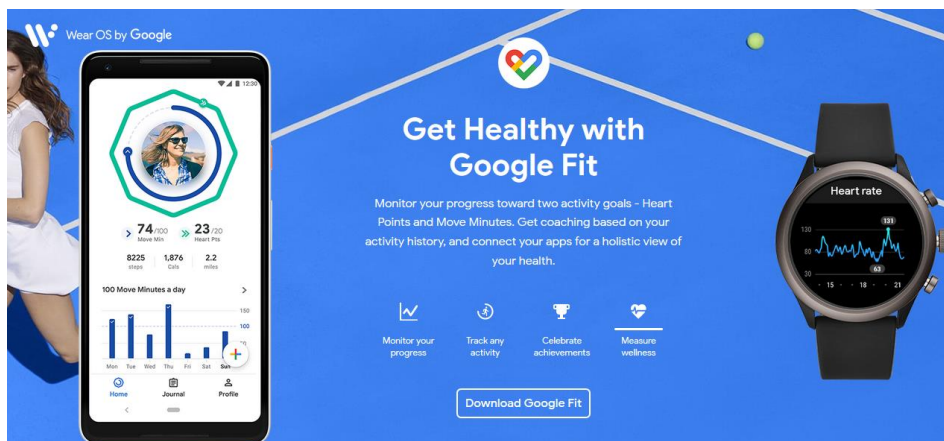


Gráfico 108: Dispositivos de Google, con Fit

**Lugares en los que estoy y estuve:** Ya se vio que en Argentina más del 90% de los usuarios de dispositivos móviles usan Android como sistema operativo. Si, de Google. Y vimos además que Android requiere para su uso y activación de características, el ingreso de una cuenta de Google. Gracias a esta cuenta (activa todo el tiempo), el dispositivo se convierte en una especie de “rastreador personal”. De hecho, Android viene con una serie de herramientas pre instaladas, las cuales en algunos casos, hasta es imposible desinstalar. Para lo cual, la recolección de información de los usuarios, es de principio a fin y sin pausa.

Estas herramientas o aplicaciones, en muchos casos se han convertido en necesidades para nuestra rutina diaria (en esto Google ha sabido hacer bien los deberes), y el sólo empleo de las mismas, permite al gigante seguir mi actividad y también mi ubicación. De hecho, para los usuarios de dispositivos móviles que no usen Android (en nuestro país menos del 9% del mercado según lo visto en el Gráfico 34), aplicaciones tales como Waze, Google Chrome, como el resto de la suite de herramientas, pueden ser descargadas e instaladas (y en la mayoría de los casos, me animo a decir sin miedo a errar, que la mayoría de los usuarios de sistema operativo iOS (iPhone) harán uso de esa posibilidad). Es decir que gran parte de estas aplicaciones, no son exclusividad de Android. Por ende, estaríamos hablando que casi el 100% de los usuarios de dispositivos móviles, emplean herramientas de Google.

Cada vez que me conecto a la red de datos móvil (3G, 4G) el teléfono envía cierta información proporcionada por el ISP (proveedor de servicios de internet) para de esa manera poder determinar la ubicación del dispositivo. Cada vez que mi teléfono se conecta a una red WiFi, de igual manera que el caso anterior, el teléfono recolecta información como para conocer la ubicación del mismo (por ejemplo la dirección IP) para luego enviarla a Google. Ni hablar si activo el GPS e inicio aplicaciones tales como Google Maps (incluido en Android) o Waze, facilito aún más la tarea de recolección.

El lector puede visualizar su ubicación actual, como la histórica desde la url (<https://myaccount.google.com/activitycontrols/location>). Allí podrá ver el mapa, con la fecha en la que se desea visualizar la ubicación. En caso de ser usuario frecuente de la aplicación maps de Google, y tener activado el GPS de manera constante como para alimentar dicha aplicación, lo que nos permitirá ver es algo como lo que muestra el Gráfico 109 (se trata sólo de una imagen para ilustrar el funcionamiento de la herramienta):

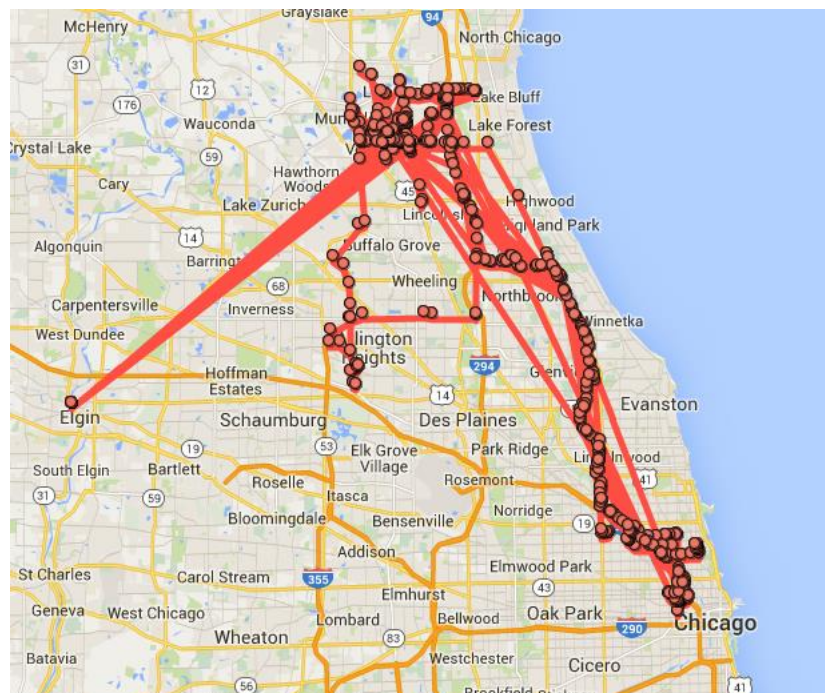


Gráfico 109: Historial de ubicación.

La configuración acerca del historial de la ubicación puede realizarse a través del panel correspondiente de la cuenta. Allí puede encontrarse una página como la que se ilustra a través del Gráfico 110 mediante la cual se nos informa como usuarios, qué información “podría” ser enviada a Google:

#### Uso y diagnóstico del Historial de ubicaciones

Quando activas el Historial de ubicaciones, tu dispositivo también puede enviar información de diagnóstico a Google sobre lo que funciona y lo que no funciona en el historial. Si activas esta configuración, puedes decidir si deseas [compartir información de uso y diagnóstico](#).

Toda la información sobre uso y diagnóstico se utiliza según la [Política de Privacidad de Google](#).

#### ¿Qué información puede compartir tu dispositivo?

Es posible que el dispositivo envíe información a Google para mejorar el Historial de ubicaciones. La información que se envía puede incluir la siguiente:

- La calidad y duración de tus conexiones con redes móviles, GPS, redes Wi-Fi o Bluetooth
- El estado de tu configuración de la ubicación
- Informes de fallas y reinicios
- Apps usadas para activar o desactivar el Historial de ubicaciones
- Niveles de batería

Gráfico 110: Historial de ubicación de Google. Información que comparte el dispositivo.

**Mi casa y mi lugar de trabajo:** De manera automática, y a través de la geolocalización de los teléfonos con sistema operativo Android, Google determina que el lugar durante el cual, el teléfono permanece aproximadamente entre 8 y 16 horas durante la noche, es nuestra casa. Y que el lugar durante el cual permanece a partir de la mañana, durante 8 horas, será la dirección de nuestro lugar de trabajo. Este análisis, tendrá un alto porcentaje de éxito en el descubrimiento de información de los usuarios. Esto es lo que describe en la nota de la revista

Forbes del año 2012 (Hill, 2012), en la cual afirma que en sólo tres días y en base a la repetición de una rutina, Google determinaba con gran porcentaje de acierto los lugares relacionados con las personas. Este aprendizaje sin duda debe estar perfeccionado en 2019.

**Mi círculo social:** A través de aplicaciones como Gmail y Hangouts (mensajería instantánea) Google conocerá los detalles de la información relacionada al intercambio de mensajes, correos electrónicos, archivos, o cualquier otro contenido con mis contactos.

- Con quién hablo con mayor frecuencia (<https://contacts.google.com/frequent>)
- A quién conozco (lista de todos mis contactos)
- Dónde me encuentro con ellos: A través de la información compartida a través de mapas, podría identificar coincidencias, patrones y saber con qué personas me reúno e interactúo. Si saco una foto que luego subo a *Google Photos* (tener en cuenta que esto podría realizarse de manera automática), podría reconocer las caras de las personas contenidas en la foto y en base a ese reconocimiento agregar las fotos en el álbum que considere corresponda (en base a las personas). Es notable cómo el algoritmo de reconocimiento, incluso puede consultarnos sobre si dos fotos de dos personas de distintas edades, corresponden a la misma persona con un altísimo nivel de exactitud. Quizás podría colocar un comentario en la foto que indique el lugar en el que fue tomada la foto, para darle aún más ayuda e información.
- Temas sobre los que intercambio mensajes. Google “lee” el contenido de nuestros correos electrónicos (Gmail) con el propósito de extraer ideas para enviar publicidad a las personas. Supuestamente, esta práctica “habría sido discontinuada” (o al menos no más con la finalidad del envío de publicidad) (Roettgers, 2017), pero dicha práctica se encuentra incluida en la declaración de “Condiciones de Servicio” vigentes de Google desde el 25 de octubre de 2017 (Condiciones de Servicio de Google, 2017). A través del Gráfico 111 se ilustra un extracto de dichas condiciones en la cual se observa:

---

☰ Google Condiciones del Servicio

---

Nuestros sistemas automatizados analizan el contenido (incluidos los correos electrónicos) para proporcionarle funciones de productos que sean relevantes para usted, como la publicación de anuncios y resultados de búsqueda personalizados y la detección de spam y software malicioso. Este análisis se realiza mientras el contenido se envía, recibe y cuando se almacena.

Gráfico 111: Condiciones de servicio de Google. Acceso al correo electrónico.

Pero en las noticias sobran muestras para saber que si no es Google quien lee nuestros mails para enviarnos anuncios, lo hacen otras empresas socias con su permiso tal como se desprende de informes de la CNN (Yurieff, 2018), y del diario The Sun (Keach, 2018).

Con lo aquí expuesto, no sólo conoce de manera individual a cada persona, sino que además tiene la capacidad de armar sus círculos sociales.

**Mis gustos y disgustos:** Con la información recolectada de mis búsquedas, de los anuncios a los cuales doy clic, Google será capaz de conocer de manera sencilla qué cosas me gustan, qué cosas elijo, qué cosas no me gustan, dónde compro, cuándo compro, mi comida preferida, los restaurants que frecuento. Tal como se describiera en párrafos anteriores, a través de una búsqueda genérica, o a través de portales específicos para realizar compras como “*Google Shopping*” (<https://www.google.com/shopping?hl=es>), “*Google Noticias*” entre otras herramientas ya mencionadas a través de las cuales podría seleccionar contenido como por ejemplo videos (YouTube). Si en alguna ocasión hice uso de “*Google Books*”, entonces tendrá registro de los libros sobre los cuales realicé algún tipo de búsqueda, para lo cual podrá recomendarme libros del mismo autor, o del mismo género. Lo mismo si a través de YouTube vi el tráiler de una película. Todo alimenta nuestro perfil el cual puede verse en <https://adssettings.google.com/>. Desde ahí uno puede configurar la manera en que desea que Google me muestre notificaciones y anuncios, y podría en caso de así desearlo, indicar que no deseo recibir anuncios relacionados con nuestras búsquedas. ¡Suerte!

Algunas de las pantallas de configuración disponibles en la cuenta de Google, a través de las cuales se informa al usuario de algunos datos menores que podría estar almacenando para hacerme la vida más fácil (¿y menos privada?):

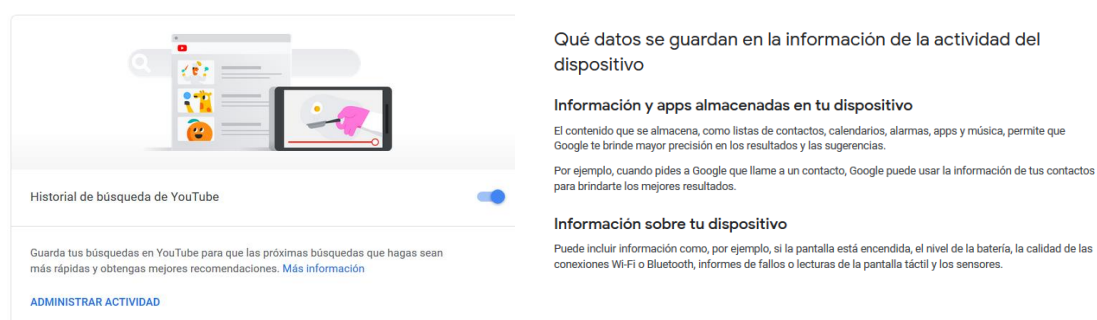


Gráfico 112: Configuración de opciones de Google.



**Mis planes y agenda:** A través del *Calendario*, (que por mi experiencia personal se trata de una herramienta muy útil y ampliamente usada no sólo en el mundo de los negocios, sino también por parte de los usuarios comunes), uno organiza eventos a los cuales invita a los participantes, quienes a su vez, confirman asistencia o no también a través de dicha herramienta. Un viaje planeado a través de búsquedas, el intercambio de correos electrónicos con agencias de viaje, con hoteles, u otros hospedajes, así como también las reservas asociadas a dichos viajes. Todo queda registrado. Con Chrome, incluso podrá saber sobre los “Likes” que dí en mis redes sociales, qué cosas tengo en mente comprar.

A través de *Google Vuelos* (<https://www.google.com/flights?hl=es>), se pueden realizar búsquedas de vuelos con parámetros tales como origen, destino, fechas, horarios, etc. Obviamente toda esa información ingresada ayudará a Google a engordar mi perfil, y por ende servirá también a la hora de enviarme anuncios y orientar futuras búsquedas.

**Mi actividad en internet:** Al emplear Chrome, Google sabrá cada movimiento realizado en la web, sitios visitados, direcciones guardadas como favoritas, tiempo de permanencia en cada sitio, documentos descargados. Todo esto permitirá, entre otras cosas, enviar publicidad con un altísimo nivel de orientación, con detalle de mis gustos, mis necesidades a mi medida. Y esta especificidad, se paga.

Sólo alcanza hacer una prueba sencilla como buscar a través del buscador de Google, cualquier bien. Por ejemplo, un lavarropa. La búsqueda nos devolverá una larga lista de direcciones, entre las cuales las primeras serán las de aquellas casas de ventas de electrodoméstico que más paguen (para posicionar mejor sus sitios). Ese posicionamiento vale, ya que generalmente los usuarios seleccionan por orden de aparición. Luego de realizar esa búsqueda, probemos cerrar el navegador, y abrir una nueva instancia de navegador, o una nueva pestaña. Ingreseemos la dirección del diario online que solemos frecuentar. La mayoría de estos diarios, tienen espacios para publicitar anuncios (de eso viven). No tardaremos en encontrar publicidad de lavarropas, de similares características a las ingresadas en el buscador hace instantes atrás.

Nuestros hábitos de navegación, orientan a Google a mostrarnos lo que nos muestra. Nada es al azar, nada es casualidad. Lo mismo al ingresar a YouTube u otras aplicaciones. Todos mis hábitos de navegación son conocidos por Google.

**Mis aplicaciones favoritas:** Esta información es muy fácil de obtener a partir de Android. Google tiene acceso absoluto a todo lo que hace el teléfono a través de ese sistema operativo: qué aplicaciones se usan, con qué frecuencia, durante cuánto tiempo, desde qué hora hasta qué

hora, TODO el detalle. Vale recordar además, que el repositorio desde el cual Android descarga las aplicaciones PlayStore, también es 100% “controlable” por Google. De hecho, las actualizaciones que se descargan e instalan desde allí en nuestro teléfono, casi que se realizan con poca o nula intervención nuestra.

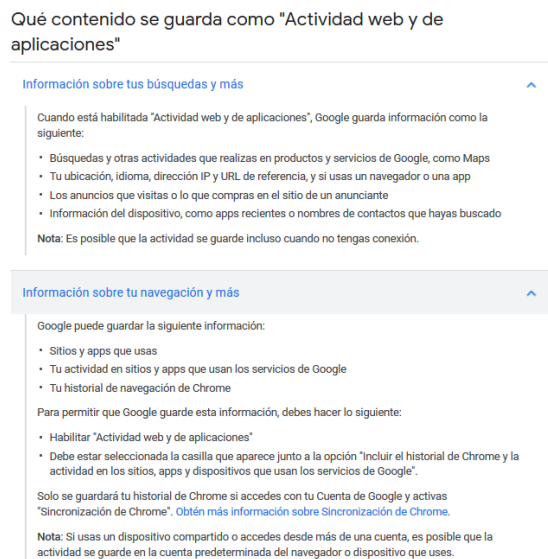


Gráfico 113: Configuración de opciones de Google sobre actividad en la web.

**Mis dispositivos:** El detalle sobre el o los dispositivos que uso con la cuenta de Google, obviamente es conocido por Google, y de hecho puede ser visualizado desde las opciones de configuración (<https://security.google.com/settings/security/activity>). Google registra dichos dispositivos, y en caso que en la lista apareciera algún dispositivo (PC, notebook, teléfono móvil, Tablet, etc) que no sea de mi pertenencia, podría ser una señal para sospechar que alguien está usando mi cuenta desde otro dispositivo. El Gráfico 114 ilustra la manera en que desde la página de configuración de Google, se muestra al usuario el conocimiento que tiene respecto a los dispositivos que se emplearon para conectarse con una determinada cuenta de usuario.

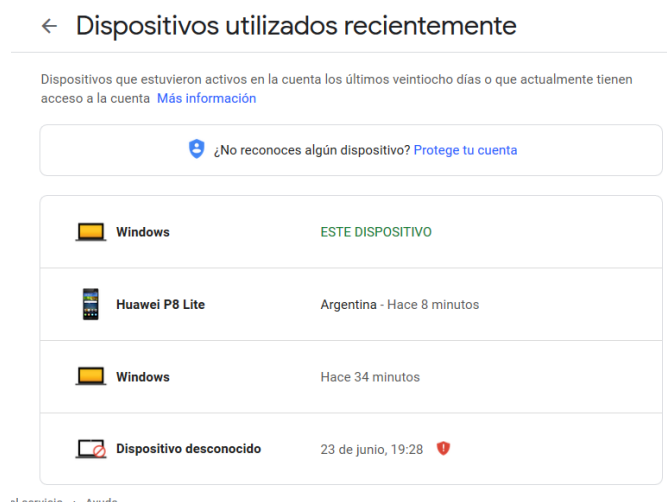


Gráfico 114: Configuración de opciones de Google. Mis dispositivos.

**Exportar mi información desde Google:** Google permite descargar toda la información que hay sobre uno de manera consolidada: marcadores de Chrome, e-mails, contactos, archivos de Google Drive, información de perfil, videos subidos a YouTube, fotos y más. Esto se realiza desde la URL: <https://www.google.com/takeout> y es una buena medida para conocer más en detalle acerca de la información que tiene de mi. El Gráfico 115 muestra la leyenda que Google ofrece al momento de indicar que se desea realizar una descarga de la información que hay disponible sobre mi:

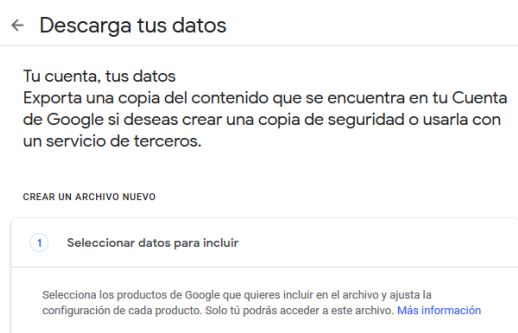


Gráfico 115: Descargar mis datos desde Google.

**Controles de actividad:** Tal como se muestra en las imágenes mostradas a través del Gráfico 116, toda la actividad que realizamos es configurable, y de hecho es altamente recomendable hacerlo:

The image shows a screenshot of the Google Activity Controls settings page. It is organized into several sections, each with a title, a brief description, and a link to 'Administrar actividad' (Manage activity). The sections are: 'Controles de actividad' (Activity Controls), 'Actividad web y de aplicaciones' (Web and app activity), 'Información del dispositivo' (Device information), 'Actividad de voz y audio' (Voice and audio activity), 'Historial de reproducciones de YouTube' (YouTube watch history), 'Historial de búsquedas de YouTube' (YouTube search history), 'Historial de ubicaciones' (Location history), 'Otra actividad' (Other activity), and 'Comentarios de "No me interesa" de YouTube' (YouTube "Not interested" comments). Each section includes a small icon and a link to manage the activity.

**Controles de actividad**

**Actividad web y de aplicaciones**

Incluye las acciones que realizas en los servicios de Google, como Maps, la Búsqueda y Play. También puede incluir lo que haces en los sitios, las apps y los dispositivos que usan los servicios de Google.

[Administrar actividad](#)

**Información del dispositivo**

Incluye tus contactos, calendarios, apps y otros datos de tus dispositivos.

[Administrar actividad](#)

**Actividad de voz y audio**

Incluye una grabación de tu voz y otros audios de los sitios, las apps y los dispositivos que usan los servicios de voz de Google.

[Administrar actividad](#)

**Historial de reproducciones de YouTube**

Incluye los videos que ves en YouTube.

[Administrar actividad](#)

**Historial de búsquedas de YouTube**

Incluye tus búsquedas de YouTube.

[Administrar actividad](#)

**Historial de ubicaciones**

Incluye los lugares que visitas con tus dispositivos (incluso cuando no usas un servicio específico de Google).

[Administrar actividad](#)

**Otra actividad**

**Comentarios de "No me interesa" de YouTube**

Los comentarios sobre "No me interesa" se usan para quitar videos de las recomendaciones de YouTube.

[Más información](#)

Borrar

Gráfico 116: Opciones para configurar controles de actividad

Allí todos los controles de actividad pueden ser personalizados para indicar una serie de parámetros tal como se indicó a lo largo de la presente sección.

Parte de la información de esta sección, toma como base las páginas de los portales "https://techengage.com" (Zahra, 2018) y de "https://thebestvpn.com" (Mardisalu, 2018).

## ANEXO IV – Argentina. Proyecto de Ley: Ley de protección de datos personales (2018).

El presente anexo presenta los detalles más significativos del Proyecto de Ley de nuestro país (Ley de Protección de Datos Personales), el cual se encuentra en el Congreso de la Nación desde el año 2018 para su evaluación.

Entre las modificaciones del Proyecto de Ley, se distinguen definiciones de conceptos tales como “datos biométricos”, “datos genéticos” entre otros. A su vez, se redefinen algunos conceptos que en la Ley vigente resultaban ambiguos en muchos casos, tales como “datos personales”, “datos sensibles”. Entre los puntos destacados, se puede citar:

- *Ámbito de aplicación* (Artículo 4). El proyecto de Ley sigue los lineamientos de la RGPD en cuanto al ámbito de aplicación. En tal sentido, dispone que la normativa se aplicará aun cuando el responsable de los datos no se encuentre en territorio nacional:
  - a- “El responsable del tratamiento se encuentre establecido en el territorio nacional, aun cuando el tratamiento de datos tenga lugar fuera de dicho territorio;
  - b- El responsable del tratamiento no se encuentre establecido en el territorio nacional, sino en un lugar en que se aplica la legislación nacional en virtud del derecho internacional;
  - c- El tratamiento de datos de titulares que residan en la REPÚBLICA ARGENTINA sea realizado por un responsable del tratamiento que no se encuentre establecido en el territorio nacional, y las actividades de dicho tratamiento se encuentren relacionadas con la oferta de bienes o servicios a dichos titulares de los datos en la REPÚBLICA ARGENTINA, o con el seguimiento de sus actos, comportamientos o intereses; excepto cuando la ley del lugar donde se encuentra el responsable del tratamiento sea más favorable para la protección del titular de los datos.”
- *Principio de finalidad* (Artículo 6) “Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines.”
- *Principio de minimización de datos* (Artículo 7). “Los datos personales deben ser tratados de manera que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron recolectados.”

- Principio de exactitud (Artículo 8). “Los datos personales deben ser tratados de modo que sean exactos y completos. Si fuera necesario adecuarlos, se adoptarán todas las medidas razonables para que se supriman o rectifiquen.”
- Plazo de conservación (Artículo 9). “Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. Los datos personales pueden conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente Ley a fin de proteger los derechos del titular de los datos.”
- Consentimiento (Artículo 12). “El tratamiento de datos, en cualquiera de sus formas, requiere del consentimiento libre e informado de su titular para una o varias finalidades específicas.”
- Revocación del consentimiento (Artículo 13). “El consentimiento puede ser revocado en cualquier momento. Dicha revocación no tiene efectos retroactivos. El responsable del tratamiento está obligado a facilitar la revocación mediante mecanismos sencillos, gratuitos y, al menos, de la misma forma por la que obtuvo el consentimiento.”
- Excepciones al consentimiento previo (Artículo 14). “No es necesario el consentimiento para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre y apellido, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, ni para el tratamiento de la información crediticia en los términos del Capítulo 6.”
- Tratamiento de datos de niñas, niños y adolescentes (Artículo 18). “En el tratamiento de datos personales de una niña, niño o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la CONVENCIÓN LOS DERECHOS DEL NIÑO y demás instrumentos internacionales que busquen su bienestar y protección integral...”

Sobre los derechos del titular de los datos personales:

- Derecho de acceso (Artículo 27). “El titular de los datos, previa acreditación de su identidad, tiene el derecho de solicitar y obtener el acceso a sus datos personales que sean objeto del tratamiento.”
- Derecho de rectificación (Artículo 29). “El titular de los datos tiene el derecho a obtener del responsable del tratamiento la rectificación de sus datos personales, cuando éstos resulten ser inexactos, falsos, errados, incompletos o no se encuentren actualizados...”

- Derecho de oposición (Artículo 30). “El titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya prestado consentimiento. El responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos.”
- Derecho de supresión (Artículo 31). “El titular de los datos tiene derecho a solicitar la supresión de sus datos personales de las bases de datos del responsable del tratamiento cuando el tratamiento no tenga un fin público, a fin de que los datos ya no estén en su posesión y dejen de ser tratados por este último...”
- Derecho a la portabilidad de datos personales (Artículo 33). “Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización...”

Sobre las obligaciones de los responsables y encargados del tratamiento de datos

- Principio de responsabilidad proactiva (Artículo 10). “El responsable o encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la autoridad de control su efectiva implementación.”
- Principio de seguridad de los datos personales (Artículo 19). “El responsable del tratamiento y, en su caso, el encargado, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.”
- Notificación de incidentes de seguridad (Artículo 20). “En caso de que ocurra un incidente de seguridad de datos personales, el responsable del tratamiento debe notificarlo a la autoridad de control sin dilación indebida y, de ser posible, dentro de las SETENTA Y DOS (72) horas de haber tomado conocimiento del incidente...”
- Protección de datos desde el diseño y por defecto (Artículo 38). “El responsable del tratamiento debe aplicar medidas tecnológicas y organizativas apropiadas tanto con

anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos establecidos en la presente Ley...”

A fin de facilitar el cumplimiento de la Ley, y siguiendo la metodología implementada por otras legislaciones (entre ellas la RGPD), se crea la figura de un funcionario especializado, bajo el título de Delegado de Protección de Datos como obligación para los responsables y encargados del tratamiento de datos:

- Delegado de Protección de Datos (Artículo 43). “Los responsables y encargados del tratamiento deben designar un Delegado de Protección de Datos en cualquiera de los siguientes supuestos:
  - a. Cuando revistan el carácter de autoridades u organismos públicos;
  - b. Se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento;
  - c. Se realice tratamiento de datos a gran escala.....”
- Se designa a la Agencia de Acceso a la Información Pública (AAIP) como autoridad de control (<https://www.argentina.gob.ar/aaip>) Según su portal “Garantizamos el derecho de acceso a la información pública, promovemos medidas de transparencia activa y la protección de los datos personales.”
- En relación con las sanciones, el Proyecto establece como referencia para cuantificar el valor de las multas el Salario Mínimo Vital y Móvil vigente al momento de su imposición.

En el sitio Informática legal (Datos Personales y Privacidad en Informática Legal) puede encontrarse información legal sobre datos personales y privacidad de la información relacionada a diversos temas específicos que no son tratados en este documento con profundidad, como ser:

- Registros y Bases de Datos Privadas
- Registros y Bases de Datos Públicas
- Datos de Salud y Datos Genéticos
- Medidas de Seguridad para el Tratamiento y Conservación de Datos Personales
- Bases de datos de marketing y publicidad
- Información obligatoria en páginas web
- Infracciones y Sanciones por incumplimiento de la Ley 25.326
- Videocámaras



- Drones o VANTs (vehículo aéreo no tripulado)
- Registro "No Llame"
- Datos Biométricos y de Identificación Personal
- Transferencia Internacional de Datos Personales
- Jurisprudencia e Información sobre Datos Personales

## ANEXO V - Cuestionario

El mismo se responde de manera totalmente anónima, y no contiene preguntas que permitan revelar la identidad del encuestado. A su vez, la información recolectada se procesa de manera agregada, y no individual. Estas pautas favorecen la buena predisposición para completar el mismo por parte de los encuestados.

Está compuesto por 16 preguntas escritas en lenguaje coloquial y de fácil comprensión. El tiempo estimado para completarla es de menos de 5 minutos y se encuentra cargado en la plataforma Google Forms.

La misma fue distribuida principalmente, a través de WhatsApp a modo de cadena (envío a grupo de contactos, y reenvío de estos últimos a sus propios contactos) y correo electrónico. La misma fue respondida por 315 personas.

### Portada con mensaje para el encuestado

A través del Gráfico 117 se ilustra la portada del cuestionario, y el mensaje que recibe el encuestado en el cual se hace referencia a la simplicidad del mismo y al tiempo que insume completarlo.

### Encuesta: Internet y la privacidad.

La siguiente encuesta contiene preguntas relacionadas al uso que hacés de las aplicaciones e internet. Está compuesta por 16 preguntas de fácil lectura y comprensión, es absolutamente anónima y no te llevará más de 5 minutos completarla.

\*Obligatorio



Gráfico 117: Portada del cuestionario.

### Agradecimiento para el encuestado

El Gráfico 118 ilustra el mensaje que recibe el encuestado al finalizar el cuestionario.

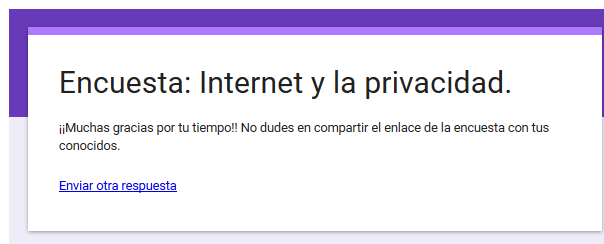


Gráfico 118: Agradecimiento al encuestado.

El cuadro siguiente brinda la lista de preguntas que conforman el cuestionario. Bajo la columna “Comentarios”, se introduce una breve leyenda que describe de manera sencilla, cuál es el objetivo de la misma, y qué es lo que se pretende obtener a partir de la respuesta por parte del encuestado.

	Pregunta	Comentarios
1	<p>Indicá tu edad *</p> <p><input type="radio"/> Menor de 18 años.</p> <p><input type="radio"/> Entre 18 y 24 años inclusive.</p> <p><input type="radio"/> Entre 25 y 34 años inclusive.</p> <p><input type="radio"/> Entre 35 y 44 años inclusive.</p> <p><input type="radio"/> Entre 45 y 54 años inclusive.</p> <p><input type="radio"/> Entre 55 y 64 años inclusive.</p> <p><input type="radio"/> Mayor de 65 años.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> Variable de control que permite evaluar el resto de las respuestas contenidas en la encuesta, discriminando por este valor.</p>
2	<p>¿Cuál de las siguientes opciones representa mejor tu género? *</p> <p><input type="radio"/> Masculino</p> <p><input type="radio"/> Femenino</p> <p><input type="radio"/> Otro</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> Variable de control que permite evaluar el resto de las respuestas contenidas en la encuesta, discriminando por este valor. Nótese que se incorpora la opción “Otro” para dar lugar a respuestas que salieran del estereotipo binario de género.</p>
3	<p>Indicá tu último nivel de estudios concluido *</p> <p><input type="radio"/> Ninguno</p> <p><input type="radio"/> Primario</p> <p><input type="radio"/> Secundario</p> <p><input type="radio"/> Universitario</p> <p><input type="radio"/> Posgrado</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> Variable de control que permite evaluar el resto de las respuestas contenidas en la</p>

		encuesta, discriminando por este valor.
4	<p>¿Qué redes sociales usás? *</p> <p><input type="checkbox"/> Instagram</p> <p><input type="checkbox"/> Facebook</p> <p><input type="checkbox"/> Twitter</p> <p><input type="checkbox"/> Pinterest</p> <p><input type="checkbox"/> WhatsApp</p> <p><input type="checkbox"/> Telegram</p> <p><input type="checkbox"/> LinkedIn</p> <p><input type="checkbox"/> Snapchat</p> <p><input type="checkbox"/> Tik Tok</p> <p><input type="checkbox"/> Redes sociales de uso anónimo (tipo Voxed)</p> <p><input type="checkbox"/> Otras que no están en la lista</p> <p><input type="checkbox"/> No uso ninguna red social</p>	<p><b>Múltiples opciones son posibles, de respuesta obligatoria.</b> La pregunta permite evaluar si se trata de un usuario activo en el ámbito de las redes sociales, y a su vez, conocer si emplea varias al mismo tiempo. La intención de la pregunta es evaluar el uso de múltiples plataformas en simultáneo, y a su vez, determinar cuáles son aquellas más y menos empleadas por el universo alcanzado.</p>
5	<p>¿Publicaste alguna vez información relacionada a alguno de los siguientes ítems? *</p> <p><input type="checkbox"/> Números telefónicos .</p> <p><input type="checkbox"/> Lugar u horario de trabajo.</p> <p><input type="checkbox"/> Información de tu casa: ubicación, fotos, etc.</p> <p><input type="checkbox"/> Fecha, lugar, fotos de donde pasás tus vacaciones.</p> <p><input type="checkbox"/> Tarjetas de débito/crédito u otros datos financieros.</p> <p><input type="checkbox"/> Nunca publico nada de lo listado.</p>	<p><b>Múltiples opciones son posibles, de respuesta obligatoria.</b> La pregunta pretende conocer qué tipo de información comúnmente considerada como sensible, suele ser publicada por los encuestados, de manera de poder determinar el nivel de consideración que se posee sobre la protección de los datos.</p>
6	<p>¿Cuáles de los siguiente datos considerarás privados? *</p> <p><input type="checkbox"/> Tu teléfono.</p> <p><input type="checkbox"/> Tu domicilio.</p> <p><input type="checkbox"/> Información sobre tus pertenencias (auto, moto, casa, ropa, etc).</p> <p><input type="checkbox"/> Tu lugar de trabajo.</p> <p><input type="checkbox"/> Información de tus horarios (de ingreso ó egreso al trabajo, a la escuela, a la facultad, al gimnasio, al club, en que te tomás el colectivo, etc).</p> <p><input type="checkbox"/> Fecha ó lugar donde pasás tus vacaciones.</p> <p><input type="checkbox"/> Información de tus tarjetas de crédito, débito u otra iformación financiera.</p> <p><input type="checkbox"/> Información relacionada a tus creencias religiosas.</p> <p><input type="checkbox"/> Información relacionada a tus convicciones políticas.</p> <p><input type="checkbox"/> Información relacionada a tu sexualidad y/ó preferencia sexual.</p>	<p><b>Múltiples opciones son posibles, de respuesta obligatoria.</b> Esta pregunta intenta contrarrestar lo que los encuestados dicen haber publicado (pregunta 5), contra lo que consideran como privado para hallar posibles contradicciones entre lo que creen que no deberían publicar, y lo que terminan publicando. A su vez, se intenta conocer cómo los encuestados evalúan temáticas, que a priori,</p>

		podrían considerarse como privadas y sensibles.
7	<p>¿Tuviste la experiencia de publicar algo en las redes de lo cual te hayas arrepentido? *</p> <p><input type="radio"/> Si.</p> <p><input type="radio"/> No.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> La pregunta tiene por fin, conocer la cantidad de encuestados que han sufrido esta experiencia. Bajo la premisa de que todo lo que se publica, queda para siempre en la red, es importante hacer foco en este punto, de manera de generar conciencia al momento de publicar contenido en la red.</p>
8	<p>¿Facilitás la ubicación a aplicaciones de tu dispositivo móvil? (permite que las aplicaciones conozcan desde dónde te estás conectando) *</p> <p><input type="radio"/> No sé de qué se trata.</p> <p><input type="radio"/> Si, siempre que se me solicita.</p> <p><input type="radio"/> Sólo a veces.</p> <p><input type="radio"/> Sólo si uso el GPS de mi dispositivo.</p> <p><input type="radio"/> Nunca.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> La pregunta tiene por fin conocer en qué grado, una funcionalidad a simple vista inofensiva, pero que recolecta muchísima información sensible de las personas, es usado por los encuestados.</p>
9	<p>¿Leíste o conocés la política de privacidad de las redes sociales que utilizás? *</p> <p><input type="radio"/> No sé de qué se trata una política de privacidad.</p> <p><input type="radio"/> No la conozco ni la leí.</p> <p><input type="radio"/> Tengo una idea de qué se trata, pensé en leerla, pero nunca lo hice.</p> <p><input type="radio"/> Tengo una idea de qué se trata, empecé a leerla, pero nunca terminé.</p> <p><input type="radio"/> Sí, la conozco y la leí.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> A partir de esta pregunta, se pretende analizar el nivel de conciencia que los encuestados poseen sobre la existencia de las políticas de privacidad que aceptan para hacer uso de las redes sociales.</p>
10	<p>¿Personalizaste las opciones de privacidad de tu perfil en redes sociales? (Por ejemplo: quien puede o no ver tu contenido ó comentar algo al respecto). *</p> <p><input type="radio"/> No sabía que existían esas opciones y que se pueden personalizar.</p> <p><input type="radio"/> No las modifiqué, las tengo como vienen por defecto.</p> <p><input type="radio"/> No las modifiqué, pero tengo intenciones de hacerlo.</p> <p><input type="radio"/> Si, las personalicé.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> La personalización de las opciones de privacidad, podría tomarse como consecuencia de, al menos, una idea</p>

		<p>de limitar potenciales riesgos a la privacidad de la información publicada. Por lo cual, puede considerarse como una señal positiva en el análisis que se pretende en la presente investigación.</p>
<p>11</p>	<p>¿Usás la misma contraseña para distintas aplicaciones? *</p> <p><input type="radio"/> Mi contraseña es la misma para todo o casi todo.</p> <p><input type="radio"/> Tengo un par de contraseñas que uso para todo, o casi todo.</p> <p><input type="radio"/> Tengo una contraseña distinta para cada aplicación que me requiere una.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> El uso de distintas contraseñas debería ser una práctica casi obligatoria. Para el caso de personas que hacen uso de gran cantidad de aplicaciones y/o dispositivos que requieran de una contraseña, existen mecanismos que aumentan la seguridad al respecto (esto excede el alcance de este documento). El uso de una única contraseña, o de pocas contraseñas para todo, es una práctica recurrente y no recomendable que es conocida por aquellas personas mal intencionadas que desean robar algún tipo de información de las potenciales víctimas. Con lo cual, esta práctica facilitará en mucho su tarea.</p>
<p>12</p>	<p>¿Conocés a alguien que haya sufrido algún episodio de robo de información (robo de contraseña, robo de tarjetas de débito/crédito, etc)? *</p> <p><input type="radio"/> Si.</p> <p><input type="radio"/> No.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> Sufrir un episodio de robo de algún tipo de información, se ha convertido en la actualidad, en algo más común de lo que muchos podrían creer. Esta pregunta intenta dejar en manifiesto esta afirmación. La información</p>

		robada podría ser algo simple y sencillo sin mayores consecuencias, o bien, podría ser algo grave con consecuencias en la vida normal de las personas.
13	<p>¿Usás redes WiFi gratuitas en la vía pública (bares, plazas, aeropuertos)? *</p> <p><input type="radio"/> Siempre que puedo.</p> <p><input type="radio"/> De vez en cuando.</p> <p><input type="radio"/> Nunca. No es una práctica a la que esté acostumbrado.</p> <p><input type="radio"/> Nunca. Me da miedo usar redes desconocidas.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> Al igual que el uso de las funcionalidades de georreferenciación, el uso de redes WiFi gratuitas es una práctica común que en general, sus usuarios suelen desconocer la infinidad de riesgos asociados. La pregunta intenta dar a conocer el nivel de conciencia que se posee sobre dichos riesgos, evaluando el grado de uso de este tipo de facilidades.</p>
14	<p>¿Tenés conocimiento de los datos acerca de tu vida cotidiana que recolecta Google? *</p> <p><input type="radio"/> No sabía que Google recolectaba información, y tampoco me importa.</p> <p><input type="radio"/> No sabía que Google recolectaba información, y me interesaría saber más al respecto.</p> <p><input type="radio"/> Sé que Google recolecta información, pero no me importa.</p> <p><input type="radio"/> Sé que Google recolecta información, y me interesaría saber más al respecto.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> La pregunta tiene por fin evaluar tanto el conocimiento de los encuestados sobre la temática abordada, como así también el nivel de preocupación/interés sobre la misma.</p>
15	<p>¿Qué pensás sobre la instalación de cámaras de video en la vía pública, y en la posibilidad que las mismas graben parte de nuestra vida diaria? *</p> <p><input type="radio"/> No me importa.</p> <p><input type="radio"/> Me parece que está bien.</p> <p><input type="radio"/> No me gusta. Me siento observado.</p> <p><input type="radio"/> No tengo una opinión al respecto.</p>	<p><b>Opciones mutuamente excluyentes, de respuesta obligatoria.</b> A través de esta pregunta, se pretende conocer en qué medida la proliferación de cámaras de video en la vía pública, repercute en la sensación de protección de las personas, y en qué medida aumenta la sensación de</p>

		“sentirse observado” como una potencial violación a la privacidad.
16	<p>Podés agregar comentarios, ideas, sugerencias o lo que te parezca en el siguiente cuadro.</p> <p><small>Tu respuesta</small></p> <hr/>	<p><b>Cuadro de texto libre, no obligatorio.</b></p> <p>Permite al encuestado escribir lo que desee.</p>



## Referencias

- ¿Cómo hace Google para ganar tanto dinero? en BBC. (27 de 03 de 2016). Obtenido de [https://www.bbc.com/mundo/noticias/2016/03/160321\\_google\\_ganancias\\_graficos\\_finde\\_dv](https://www.bbc.com/mundo/noticias/2016/03/160321_google_ganancias_graficos_finde_dv)
- ABC - San Francisco, reconocimiento facial. (15 de 05 de 2019). Obtenido de [https://www.abc.es/sociedad/abci-san-francisco-prohibe-policia-usar-tecnicas-reconocimiento-facial-201905151430\\_noticia.html](https://www.abc.es/sociedad/abci-san-francisco-prohibe-policia-usar-tecnicas-reconocimiento-facial-201905151430_noticia.html)
- ABC - Yahoo Robo de información. (25 de 09 de 2017). Obtenido de [https://www.abc.es/tecnologia/redes/abci-hackeo-yahoo-incluye-datos-funcionarios-alto-nivel-eeuu-sido-venidos-deep-201612161851\\_noticia.html](https://www.abc.es/tecnologia/redes/abci-hackeo-yahoo-incluye-datos-funcionarios-alto-nivel-eeuu-sido-venidos-deep-201612161851_noticia.html)
- Aiello, C. (22 de 08 de 2018). CNBC - Chip en empleados. Obtenido de <https://www.cnbc.com/2018/08/22/three-square-market-plans-gps-chip-dementia-patients.html>
- Aldama, Z. (27 de 04 de 2018). El País - Videovigilancia China. Obtenido de [https://retina.elpais.com/retina/2018/04/25/tendencias/1524640135\\_207540.html](https://retina.elpais.com/retina/2018/04/25/tendencias/1524640135_207540.html)
- Álvarez, R. (09 de 02 de 2018). Xataka - Monitoreo China. Obtenido de <https://www.xataka.com/privacidad/20-millones-de-camaras-equipadas-con-inteligencia-artificial-hacen-que-china-sea-el-verdadero-gran-hermano>
- Amnistía Internacional. (04 de 12 de 2019). Obtenido de <https://www.amnesty.org/es/latest/news/2019/12/big-tech-privacy-poll-shows-people-worried>
- Ansorena, J. (03 de 05 de 2018). ABC - Cierre Cambridge Analytica. Obtenido de [https://www.abc.es/tecnologia/redes/abci-cambridge-analytica-anuncia-cierre-tras-escandalo-filtracion-datos-personales-facebook-201805022037\\_noticia.html](https://www.abc.es/tecnologia/redes/abci-cambridge-analytica-anuncia-cierre-tras-escandalo-filtracion-datos-personales-facebook-201805022037_noticia.html)
- Ansorena, J. (11 de 04 de 2018). ABC - Zuckerberg Congreso. Obtenido de [https://www.abc.es/tecnologia/redes/abci-sigue-directo-comparecencia-zuckerberg-congreso-estados-unidos-201804111529\\_directo.html](https://www.abc.es/tecnologia/redes/abci-sigue-directo-comparecencia-zuckerberg-congreso-estados-unidos-201804111529_directo.html)
- Argentina - Constitución Nacional. (15 de 12 de 1994). Obtenido de <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm>
- Argentina - Ley 25.326. (10 de 2000). Obtenido de <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>
- Argentina - Mobile Network Experience Report. (06 de 2019). Obtenido de <https://www.opensignal.com/reports/2019/06/argentina/mobile-network-experience>

- Argentina Ciber Segura - Guía sobre Privacidad.* (s.f.). Obtenido de [https://www.argentinacibersegura.org/admin/resources/files/consejos/33/Gu%C3%A1Da\\_sobre\\_Privacidad.pdf](https://www.argentinacibersegura.org/admin/resources/files/consejos/33/Gu%C3%A1Da_sobre_Privacidad.pdf)
- Ball, J. (20 de 11 de 2013). *The Guardian - Vigilancia Snowden.* Obtenido de <https://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>
- Ball, J. (27 de 01 de 2014). *The Guardian - Angry Birds...* Obtenido de <https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data>
- Barranco Fragoso, R. (18 de 06 de 2012). *Big Data - IBM.* Obtenido de <https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html>
- BBC - ISPs en EEUU.* (29 de 03 de 2017). Obtenido de <https://www.bbc.com/mundo/noticias-39431051>
- BBC - Monitoreo en China.* (26 de 12 de 2017). Obtenido de <https://www.bbc.com/mundo/noticias-internacional-42398920>
- BBC - Multa Facebook.* (24 de 07 de 2019). Obtenido de <https://www.bbc.com/mundo/noticias-49093124>
- Belshaw, D. (12 de 2017). *Privacy vs Security.* Obtenido de <https://wikity.readwriterespond.com/privacy-vs-security/>
- Brasil - Ley 12737/12.* (30 de 11 de 2012). Obtenido de [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm)
- Brasil - Ley 12965.* (23 de 04 de 2014). Obtenido de [http://www.planalto.gov.br/CCIVIL\\_03/\\_Ato2011-2014/2014/Lei/L12965.htm](http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm)
- Brasil - Ley 13709/18.* (14 de 08 de 2018). Obtenido de [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)
- Brooker, C. (Dirección). (2011). *Black Mirror* [Película].
- Browser Market Share Argentina en Statcounter.* (07 de 2019). Obtenido de <http://gs.statcounter.com/browser-market-share/all/argentina>
- Browser Market Share worldwide en Statcounter.* (07 de 2019). Obtenido de <http://gs.statcounter.com/browser-market-share>
- Cadwalladr, C., & Graham-Harrison, E. (17 de 03 de 2018). *The Guardian - Cambridge Analytica - Facebook.* Obtenido de <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

- Canadá - Ley PIPEDA. (13 de 04 de 2000). Obtenido de <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html>
- Cejas, E. B., & González, C. C. (2015). 44 JAIIO - Normativa video vigilancia. Obtenido de <http://44jaiio.sadio.org.ar/sites/default/files/sid174-184.pdf>
- Chile - Boletín Proyecto de Ley 11092-07. (06 de 07 de 2018). Obtenido de [https://www.camara.cl/pley/pley\\_detalle.aspx?prmID=11608&prmBoletin=11092-07](https://www.camara.cl/pley/pley_detalle.aspx?prmID=11608&prmBoletin=11092-07)
- Chile - Boletín proyecto de Ley 11144-07. (06 de 07 de 2018). Obtenido de [https://www.camara.cl/pley/pley\\_detalle.aspx?prmID=11661&prmBoletin=11144-07](https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07)
- Chile - Ley 19628. (28 de 08 de 1999). Obtenido de <https://www.leychile.cl/Navegar?idNorma=141599>
- Chile - Ley 21.096. (16 de 06 de 2018). Obtenido de <https://www.leychile.cl/Navegar?idNorma=1119730>
- Colombia - Ley 1.266. (31 de 12 de 2018). Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>
- Colombia - Ley 1.581. (17 de 10 de 2012). Obtenido de <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Colombia - Portal Dejusticia. (2019). Obtenido de <https://www.dejusticia.org/acerca-de-nosotros/>
- Colombia - Proyecto de Ley 089. (2017). Obtenido de <http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2017-2018/980-proyecto-de-ley-089-de-2017>
- Concejo Deliberante La Plata. (20 de 12 de 2017). Obtenido de <http://www.concejodeliberante.laplata.gov.ar/digesto/or12000/or11623.html>
- Condiciones de Servicio de Google. (25 de 10 de 2017). Obtenido de <https://policies.google.com/terms>
- Corrales, G. (30 de 08 de 2015). La Nación - Caso Ashley Madison. Obtenido de <https://www.nacion.com/tecnologia/internet/el-caso-ashley-madison-el-hackeo-que-desnudo-a-39-millones-de-infieles/7QWUS3A4SNDQDLICN4YJANGGHU/story/>
- Data Never Sleeps 7.0 en Domo. (s.f.). Obtenido de <https://www.domo.com/learn/data-never-sleeps-7>
- Datos Personales y Privacidad en Informática Legal. (s.f.). Obtenido de <http://www.informaticalegal.com.ar/legislacion-informatica/datos-personales/>
- Defensoría del Pueblo de la Ciudad de Buenos Aires. (22 de 01 de 2019). Defensoría del Pueblo GCBA - Fake News. Obtenido de

- <https://www.facebook.com/DefensoriaCABA/videos/elecciones-2019-c%C3%B3mo-detectar-una-noticia-falsa-o-fake-news/315364472664887/>
- del Castillo, M. (06 de 09 de 2017). *Hackear un coche puede estar al alcance de cualquiera en Autopista*. Obtenido de <https://www.autopista.es/tecnologia/articulo/hackear-coche-alcance-cualquiera>
- Diario Ámbito - Centro de Monitoreo La Plata*. (2019). Obtenido de <https://www.ambito.com/la-plata-inauguran-nuevo-centro-monitoreo-cameras-seguridad-inteligentes-n5033119>
- Díaz, A. (28 de 06 de 2017). *Blogthinkbig - Chip en empleados*. Obtenido de <https://empresas.blogthinkbig.com/tecnologia-y-privacidad/>
- Díaz, I. (18 de 05 de 2017). *Forbes - Las razones por las que la privacidad...* Obtenido de <https://forbes.es/empresas/10946/las-razones-por-las-que-la-privacidad-es-importante-para-su-negocio-su-marca-y-su-futuro/>
- Diccionario de la Real Academia Española - Información*. (s.f.). Obtenido de <https://dle.rae.es/?w=informaci%C3%B3n>
- Diccionario de la Real Academia Española - Privacidad*. (s.f.). Obtenido de <https://dle.rae.es/?w=privacidad>
- Digital 2019 en Argentina*. (31 de 01 de 2019). Obtenido de <https://datareportal.com/reports/digital-2019-argentina>
- Dispositivos de Google con Google Fit*. (2019). Obtenido de <https://wearos.google.com/#stay-healthy>
- Erice Oronoz, M. (10 de 04 de 2018). *ABC - Zuckerberg Senado*. Obtenido de [https://www.abc.es/tecnologia/abci-siga-directo-intervencion-zuckerberg-senado-eeuu-201804102104\\_noticia.html](https://www.abc.es/tecnologia/abci-siga-directo-intervencion-zuckerberg-senado-eeuu-201804102104_noticia.html)
- Estándares RIPDD*. (20 de 06 de 2017). Obtenido de [https://www.infoem.org.mx/doc/publicaciones/EPDPEI\\_2017.pdf](https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf)
- Facebook - Condiciones de Servicio*. (19 de 04 de 2018). Obtenido de <https://www.facebook.com/terms.php>
- Facebook - Política de Datos*. (18 de 04 de 2018). Obtenido de <https://www.facebook.com/about/privacy/update>
- Fernández, R. (02 de 05 de 2019). *Ingresos anuales de Google en Statista*. Obtenido de <https://es.statista.com/estadisticas/635551/google-ingresos-mundiales-anuales/>
- Freedom on the Net - Argentina*. (s.f.). Obtenido de <https://freedomhouse.org/report/freedom-net/2018/argentina>

- Freedom on the Net 2018 Map.* (s.f.). Obtenido de <https://freedomhouse.org/report/freedom-net/freedom-net-2018/map>
- Freedom on the Net Countries.* (s.f.). Obtenido de <https://freedomhouse.org/report/countries-net-freedom-2018>
- Gavetti, J.-H. (02 de 08 de 2018). *La Cloud Act, una amenaza para la privacidad... por El País.* Obtenido de [https://retina.elpais.com/retina/2018/08/01/tendencias/1533121170\\_040578.html](https://retina.elpais.com/retina/2018/08/01/tendencias/1533121170_040578.html)
- GCBA - *Reconocimiento Facial.* (2019). Obtenido de <https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos>
- GDPR Key Changes.* (s.f.). Obtenido de <https://eugdpr.org/the-regulation/>
- Gellman, B., & Poitras, L. (07 de 06 de 2013). *Washington Post - U.S., British intelligence mining data...* Obtenido de [http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story\\_1.html](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html)
- Gestión de reputación online.* (2019). Obtenido de <https://www.gestiondereputaciononline.com>
- Global Digital - Enero 2019.* (01 de 2019). Obtenido de <https://wearesocial.com/global-digital-report-2019>
- Global Digital - Julio 2019.* (07 de 2019). Obtenido de <https://datareportal.com/reports/digital-2019-internet-trends-in-q3>
- Global Digital - Octubre 2019.* (10 de 2019). Obtenido de <https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-october-2019>
- Goel, S., Miesing, P., & Chandra, U. (2010). *The Impact of Illegal Peer-to-Peer File-Sharing on the Media Industry.* Obtenido de <https://journals.sagepub.com/doi/pdf/10.1525/cmr.2010.52.3.6>
- Google Home.* (s.f.). Obtenido de [https://store.google.com/es/product/google\\_home](https://store.google.com/es/product/google_home)
- Greenberg, A. (08 de 01 de 2016). *The Jeep Hackers Are Back en Wired.* Obtenido de <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>
- Greenwald, G., & MacAskill, E. (07 de 06 de 2013). *The Guardian - NSA Prism program taps in to user data of Apple, Google and others.* Obtenido de <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>
- Guimón, P. (03 de 05 de 2018). *El País - Cierre Cambridge Analytica.* Obtenido de [https://elpais.com/internacional/2018/05/02/actualidad/1525285885\\_691249.html](https://elpais.com/internacional/2018/05/02/actualidad/1525285885_691249.html)

- Gupta, A. (16 de 04 de 2019). *Países con bloqueos - The Windows Club*. Obtenido de <https://www.thewindowsclub.com/list-of-countries-that-have-banned-social-media-for-its-citizens>
- Heather, K. (30 de 06 de 2018). *California aprueba la ley de privacidad... en CNN*. Obtenido de <https://cnnespanol.cnn.com/2018/06/30/california-ley-privacidad-internet-estricta-estados-unidos/>
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la investigación*. México D.F.: McGraw-Hill.
- Hill, K. (09 de 07 de 2012). *It Takes Google 'Now' Three Days To Figure Out Where You Live*. Obtenido de <https://www.forbes.com/sites/kashmirhill/2012/07/09/it-takes-google-now-three-days-to-figure-out-where-you-live/#35212caf7d68>
- Información en Wikipedia*. (29 de 07 de 2019). Obtenido de <https://es.wikipedia.org/wiki/Informaci%C3%B3n>
- Informe Comité Jurídico Interamericano*. (26 de 03 de 2015). Obtenido de [http://www.oas.org/es/sla/ddi/docs/CJI-doc\\_474-15\\_rev2.pdf](http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf)
- IoT - Crecimiento de dispositivos conectados a la red*. (2019). Obtenido de <https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/>
- Isaac, M., Benner, K., & Frenkel, S. (22 de 11 de 2017). *NYT - Hackeo Uber*. Obtenido de <https://www.nytimes.com/es/2017/11/22/uber-hackeo-rescate-datos/>
- Jaimovich, D. (15 de 07 de 2019). *Infobae*. Obtenido de <https://www.infobae.com/america/tecno/2019/07/15/los-riesgos-de-conectarse-a-una-wifi-publica/>
- Keach, S. (21 de 09 de 2018). *MAIL FAIL Google admits it still lets HUNDREDS of companies read your Gmail emails*. Obtenido de <https://www.thesun.co.uk/tech/7312296/google-read-gmail-emails-snoop/>
- Ley UE 2016/679 - RGPD*. (27 de 04 de 2016). Obtenido de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- Mardisalu, R. (09 de 07 de 2018). *What Does Google Know About You: A Complete Guide*. Obtenido de <https://thebestvpn.com/what-does-google-know-about-you/>
- Mármol, H. (30 de 05 de 2019). *... primera prueba de la red 5G en Argentina*. Obtenido de [https://www.clarin.com/tecnologia/personal-huawei-realizaron-primera-prueba-red-5g-argentina\\_0\\_ERkZMBI9H.html](https://www.clarin.com/tecnologia/personal-huawei-realizaron-primera-prueba-red-5g-argentina_0_ERkZMBI9H.html)

- Martí, A. (13 de 04 de 2017). *Filtración de Wikileaks sobre la CIA en Xataka*. Obtenido de <https://www.xataka.com/seguridad/la-mayor-filtracion-de-wikileaks-sobre-la-cia-casi-9-000-documentos-sobre-espionaje-con-smart-tvs-smartphones-y-otros>
- Maza, C. (22 de 03 de 2018). *El Confidencial - Cambridge Analytica y Brexit*. Obtenido de [https://www.elconfidencial.com/mundo/2018-03-22/cambridge-analytica-brexit-trump-farage-bannon\\_1539452/](https://www.elconfidencial.com/mundo/2018-03-22/cambridge-analytica-brexit-trump-farage-bannon_1539452/)
- Méndez, F. (03 de 09 de 2015). *Forbes - Obama Big Data*. Obtenido de <http://forbes.es/emprendedores/7560/como-el-big-data-ayudo-a-obama-a-ganar/>
- Metz, R. (17 de 08 de 2018). *Technology Review - Chip en empleados*. Obtenido de <https://www.technologyreview.com/s/611884/this-company-embeds-microchips-in-its-employees-and-they-love-it/>
- México - Ley LFPDPPP. (05 de 06 de 2010). Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>
- México - Ley LGPDPSO. (26 de 01 de 2017). Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPSO.pdf>
- Mobile Operating System Market Share Argentina en Statcounter*. (07 de 2019). Obtenido de <http://gs.statcounter.com/os-market-share/mobile/argentina>
- Mobile Operating System Market Share WorldWide en Statcounter*. (07 de 2019). Obtenido de <http://gs.statcounter.com/os-market-share/mobile/worldwide>
- Municipio de La Plata - Monitoreo*. (2019). Obtenido de <https://www.laplata.gov.ar/#/gobierno/programa/ejes?categoria=monitoreo>
- Newman Pont, V., & Ángel Arango, M. (01 de 2019). *Colombia - Documento Dejusticia*. Obtenido de <https://cdn.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf>
- Noujaim, J., & Amer, K. (Dirección). (2019). *Nada es privado (The great hack)* [Película].
- NYT - Yahoo Robo de información. (s.f.). Obtenido de [https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?ref=technology&\\_r=0](https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?ref=technology&_r=0)
- Overly, S. (08 de 03 de 2017). *Car hacking CIA, Wikileaks en The Washington Post*. Obtenido de <https://www.washingtonpost.com/news/innovations/wp/2017/03/08/what-we-know-about-car-hacking-the-cia-and-those-wikileaks-claims/?noredirect=on>
- Perú - Ley 29.733. (03 de 07 de 2011). Obtenido de <https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf>
- Poitras, L. (Dirección). (2014). *Citizenfour* [Película]. Obtenido de Citizenfour

- Portal ADC.* (2019). Obtenido de <https://adcdigital.org.ar/acerca-de/>
- Pozzi, S. (24 de 07 de 2019). *El País - Multa Facebook.* Obtenido de [https://elpais.com/economia/2019/07/24/actualidad/1563983967\\_275285.html](https://elpais.com/economia/2019/07/24/actualidad/1563983967_275285.html)
- Privacidad en Internet en Wikipedia.* (20 de 07 de 2019). Obtenido de [https://es.wikipedia.org/wiki/Privacidad\\_en\\_Internet](https://es.wikipedia.org/wiki/Privacidad_en_Internet)
- Privacy International.* (s.f.). Obtenido de <https://privacyinternational.org/es>
- Productos de Google.* (s.f.). Obtenido de <https://about.google/intl/en/products/>
- Protalinski, E. (07 de 05 de 2019). *Android passes 2.5 billion monthly active devices.* Obtenido de <https://venturebeat.com/2019/05/07/android-passes-2-5-billion-monthly-active-devices/>
- Proyecto de Ley: LEY DE PROTECCIÓN DE DATOS PERSONALES.* (09 de 2018). Obtenido de [https://www.argentina.gob.ar/sites/default/files/mensaje\\_ndeg\\_147-2018\\_datos\\_personales.pdf](https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf)
- Querido, L. (s.f.). *Transparencia Electoral - Fake news.* Obtenido de <https://www.transparenciaelectoral.org/que-medidas-se-pueden-promover-para-combatir-la-influencia-de-las-fake-news-en-las-elecciones/>
- RAE - Red Social.* (s.f.). Obtenido de <https://dej.rae.es/lema/red-social>
- Rainie, L. (27 de 03 de 2018). *Pew Research Center.* Obtenido de <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>
- Reputación Online en Wikipedia.* (02 de 08 de 2019). Obtenido de [https://es.wikipedia.org/wiki/Reputaci%C3%B3n\\_online](https://es.wikipedia.org/wiki/Reputaci%C3%B3n_online)
- Riesgos asociados a las redes Wi-Fi públicas - ESET.* (05 de 01 de 2019). Obtenido de <https://www.welivesecurity.com/la-es/2019/02/05/riesgos-asociados-redes-wi-fi-publicas/>
- Robo de datos Equifax en Infotechnology.* (08 de 09 de 2017). Obtenido de <https://www.infotechnology.com/negocios/Como-paso-y-que-podes-esperar-del-mayor-robo-de-datos-de-la-historia-financiera-20170908-0001.html>
- Roettgers, J. (23 de 06 de 2017). *Google Will Keep Reading Your Emails, Just Not for Ads.* Obtenido de <https://variety.com/2017/digital/news/google-gmail-ads-emails-1202477321/>
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (20 de 13 de 2018). *NY Times - Cambridge Analytica - Facebook.* Obtenido de <https://www.nytimes.com/es/2018/03/20/cambridge-analytica-facebook/>



- Rusbridger, A., MacAskill, E., & Gibson, J. (21 de 05 de 2015). *The Guardian - Edward Snowden*. Obtenido de <https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video>
- Saiz, E. (07 de 06 de 2013). *El País - EE UU accede a información...* Obtenido de [https://elpais.com/internacional/2013/06/07/actualidad/1370564066\\_752776.html](https://elpais.com/internacional/2013/06/07/actualidad/1370564066_752776.html)
- Scherer, M. (07 de 11 de 2012). *Revista TIME - Obama y el Big Data*. Obtenido de <http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helped-obama-win/>
- Scott, M. (31 de 07 de 2019). *Politico - Cambridge Analytica y Brexit*. Obtenido de <https://www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/>
- Scully, P. (25 de 01 de 2018). Obtenido de <https://iot-analytics.com/global-overview-1600-enterprise-iot-projects/>
- Segran, E. (11 de 04 de 2014). *Fast Company - The Truth About Teenagers, The Internet, And Privacy*. Obtenido de <https://www.fastcompany.com/3037962/the-truth-about-teenagers-the-internet-and-privacy>
- Seguridad de la Información en Wikipedia*. (04 de 08 de 2019). Obtenido de [https://es.wikipedia.org/wiki/Seguridad\\_de\\_la\\_informaci%C3%B3n](https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n)
- Serrato, J., Cwalina, C., Rudawski, A., Coughlin, T., & Fardelmann, K. (09 de 07 de 2018). *Data Protection Report - Estados que modificaron legislación*. Obtenido de <https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/>
- Society, I. (10 de 2015). *Introducción a la privacidad en Internet*. Obtenido de <https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-Privacy-20151030-es.pdf>
- Steinberg, S. (13 de 10 de 2019). *CNBC - Cyberattacks now cost companies...* Obtenido de <https://www.cnn.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>
- Stone, O. (Dirección). (2016). *Snowden* [Película].
- Taratuto, J. (Dirección). (2015). *Papeles en el viento* [Película]. Argentina.
- Ucciferri, L. (23 de 05 de 2019). *ADC Digital: #ConMiCaraNo*. Obtenido de <https://adcdigital.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/>
- Uruguay - Ley 18331*. (18 de 08 de 2008). Obtenido de <https://www.impo.com.uy/bases/leyes/18331-2008/29>

- Uruguay - Ley 19670. (25 de 10 de 2018). Obtenido de <https://www.impo.com.uy/bases/leyes/19670-2018>
- Uruguay - Nueva legislación de datos personales. (25 de 01 de 2019). Obtenido de <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/cambios-recientes-legislacion-sobre-proteccion-de-datos-personales-en>
- Vercelli, A. (09 de 2018). *SEDICI - Análisis del caso Facebook - Cambridge Analytica*. Obtenido de <http://sedici.unlp.edu.ar/handle/10915/71755>
- Visa para viajar a Estados Unidos.... en Clarín. (02 de 06 de 2019). Obtenido de [https://www.clarin.com/viajes/visa-viajar-unidos-gobierno-pedira-historial-redes-sociales-solicitantes\\_0\\_t3CHk9RkA.html](https://www.clarin.com/viajes/visa-viajar-unidos-gobierno-pedira-historial-redes-sociales-solicitantes_0_t3CHk9RkA.html)
- Weir, P. (Dirección). (1998). *The Truman Show* [Película].
- Ximénez de Sandoval, P. (26 de 09 de 2018). *El País - Hackeo Uber*. Obtenido de [https://elpais.com/tecnologia/2018/09/26/actualidad/1537985444\\_973720.html](https://elpais.com/tecnologia/2018/09/26/actualidad/1537985444_973720.html)
- Yurieff, K. (20 de 09 de 2018). *Google still lets third-party apps scan your Gmail data*. Obtenido de <https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html>
- Zahra, A. (22 de 12 de 2018). *What Google knows about you might give you goosebumps*. Obtenido de <https://techengage.com/what-google-knows-about-me/>