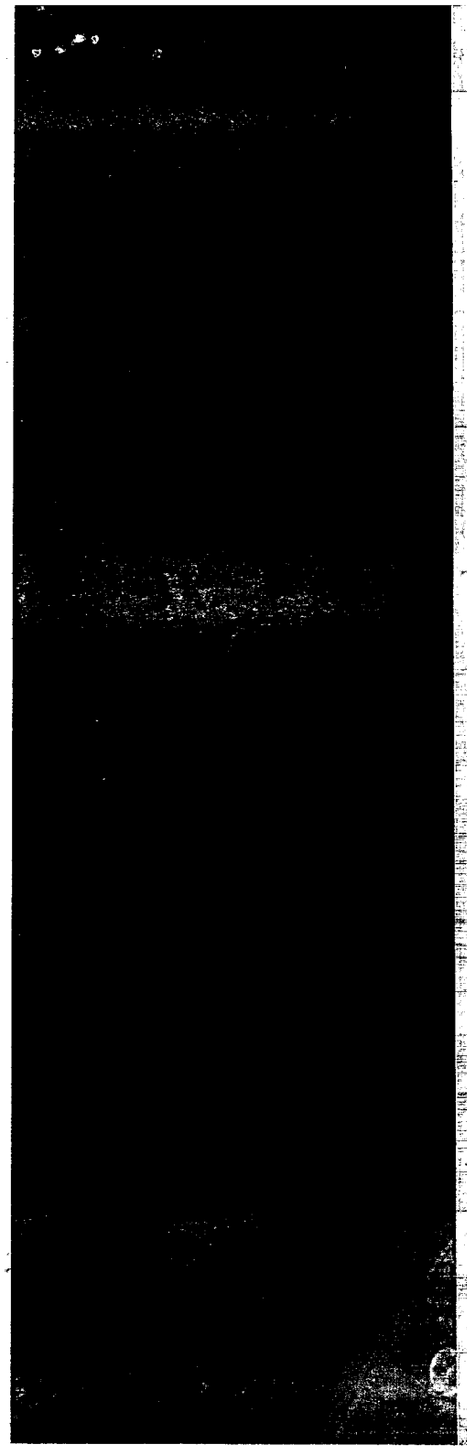


consentimiento del fiscal, el tribunal podrá suspender la realización del juicio".

"Si el delito o alguno de los delitos que integran el concurso estuviera reprimido con pena de multa aplicable en forma conjunta o alternativa con la de prisión, será condición, además, que se pague el mínimo de la multa correspondiente.

"El imputado deberá abandonar en favor del Estado Nacional los bienes que presumiblemente resultarían decomisados en caso de que recayera condena.

"No procederá la suspensión del juicio a prueba cuando un funcionario público, en el ejercicio de sus funciones, hubiese participado en el delito o se trate de un delito reprimido con pena de inhabilitación.

"Tampoco procederá la suspensión del juicio a prueba respecto de los ilícitos reprimidos por las leyes 22415 y 24769 y sus respectivas modifs.".

Art. 21.– Comuníquese al Poder Ejecutivo Nacional.

Amado Boudou (ministro de Economía y Finanzas Públicas).

Derecho Penal, Contravencional y de Faltas

Injerencias arbitrarias del Estado en los nuevos espacios de la vida privada de las personas. Alcances y fundamentos de la protección constitucional de los datos almacenados en los aparatos de telefonía celular de última generación

Por Matías Becerra y Octavio Paganelli (*)

SUMARIO: I. Introducción: la revolución en las telecomunicaciones y los nuevos ámbitos de intimidad. Aparición de los "*smartphones*".– II. ¿La información almacenada en un "*smart-phone*" puede considerarse comprendida dentro del derecho constitucional a la intimidad? La expectativa de privacidad del ciudadano.– III. ¿Qué normas constitucionales permiten construir la inviolabilidad de estos nuevos espacios íntimos?.– IV. ¿El Estado argentino está dispuesto a reconocerle al individuo su expectativa de mantener bajo reserva el contenido de su teléfono móvil?.– V. Consecuencias de nuestra postura y su confrontación con la regulación existente en los Códigos Procesales de la Nación y de la Ciudad Autónoma de Buenos Aires.– VI. Conclusiones: la regla de exclusión de prueba ilícita

I. INTRODUCCIÓN: LA REVOLUCIÓN EN LAS TELECOMUNICACIONES Y LOS NUEVOS ÁMBITOS DE INTIMIDAD. APARICIÓN DE LOS "*SMARTPHONES*"

A modo de introito es menester realizar algunas aclaraciones que si bien parecerán obvias al lector, nos permitirá comenzar a desarrollar algunas de las reflexiones que inspiraron este breve ensayo.

En los últimos años se produjo en el mundo lo que podríamos llamar la "revolución informática o telemática", debido a los notables avances en el área de la tecnología aplicada a los medios de comunicación. Existe frondosa literatura que considera al fenómeno como la segunda o tercera de las revoluciones que han tenido lugar en la historia universal del hombre, únicamente precedidas por la Francesa e Industrial de finales del siglo XVIII y principios del siglo XIX, respectivamente.

(*) Agradecemos especialmente a los Dres. Guillermo E. Morosi, Gustavo Garibaldi, Guillermo E. Friele y Pía Paganelli por las valiosas observaciones realizadas a cada una de las ideas desarrolladas en este breve ensayo.

Habida cuenta de que el estudio de los alcances de esta explosión tecnológica excede los acotados límites del presente ensayo, hemos optado por realizar una pequeña reseña de los avances en materia de la telefonía móvil, resaltando brevemente las principales diferencias entre los primeros –y hoy ya vetustos– teléfonos celulares y los actuales, en especial, los de última y avanzada tecnología denominados "*smartphones*" (teléfonos inteligentes), cuya aparición puede remontarse a finales de la década de los noventa.

En rigor, el concepto de las comunicaciones móviles aparece por primera vez en los años 1947/1960, dentro de los laboratorios de la empresa norteamericana Bell. En razón de su elevado costo, esa nueva tecnología fue utilizada originariamente por las agencias estatales para desarrollar misiones militares, y en menor medida, por algunas grandes empresas comerciales. Recién en el año 1973, aproximadamente, un ingeniero graduado en el Instituto de Tecnología del Estado de Illinois, que años antes había servido en las fuerzas navales de los Estados Unidos de Norteamérica, logró realizar la primera llamada desde un teléfono móvil en la ciudad de Nueva York mientras trabajaba para Motorola. Así, Martín Cooper se convirtió en el padre de este nuevo modo de comunicación que, a la postre, se expandiría de forma masiva hasta penetrar totalmente en la vida cotidiana de los hombres (1).

Ahora bien, para ese entonces estos teléfonos móviles contaban con una única y básica función –comunicación de voz con otra persona–, por lo que no quedaban registradas las llamadas que se realizaban o se recibían en el aparato. Por el contrario, en la actualidad es sabido que cualquier equipo inteligente de telefonía celular, hasta el modelo menos moderno, registra en su memoria las llamadas entrantes y salientes del aparato como así también su duración, posee además una agenda telefónica y otorga la posibilidad de enviar y recibir mensajes de texto (*pager*) de familiares, amigos y/o compañeros de trabajo.

En ese sentido, justo es reconocer que dicho elenco de aplicaciones ha crecido exponencialmente con la aparición de la nueva generación de "*smartphones*". En efecto, y sin perjuicio de las particularidades de los modelos que existen hoy en el mercado, puede decirse que, en líneas generales, buena parte de ellos poseen las funciones que se detallan a continuación, a saber: llamadas telefónicas de voz a otro celular, intercambio de mensajería de texto, servicio de correo electrónico instantáneo (hasta diez cuentas de correo electrónico para acceder), sistema propio de mensajería instantánea, cámara fotográfica y de video, reproductor multimedia (música, imágenes, videos, notas de voz, etcétera), agenda, libreta de notas, lista de tareas, soporte para archivos adjuntos (*openoffice*, imágenes), GPS –sistema de posicionamiento global–, *bluetooth*, conexión *Wi-Fi* a internet, etcétera.

Existen teléfonos celulares con aplicaciones aún más avanzadas que permiten a los usuarios, por ejemplo, acceder y realizar movimientos *online* de sus cuentas bancarias (2), otros contienen dispositivos de seguridad contra hurtos y/o robos de vehículos (desde el celular se desactiva la energía del rodado durante el curso de un robo de automotor, o bien incluyen un sistema que facilita su rastreo posterior), y también, según pudimos relevar, incluyen la función de *baby call* (3); y, por último, existen otros teléfonos que incluso permiten al usuario operar, en forma de control remoto, ciertos objetos (*vgr.*, electrodomésticos y sistemas de alarma de casas y vehículos).

En definitiva, tal y como el lector apreciará sin mayor esfuerzo, muchas esferas trascendentes de la vida del hombre se encuentran "ordenadas" y/o "disciplinadas" en función de las aplicaciones de *software* de estos aparatos, situación que –y a no dudarlo– debería merecer algún tipo de protección cuando cualquier agencia u órgano del sistema penal decida compulsivamente acceder a la información allí almacenada para esclarecer un hecho ilícito de cualquier índole.

Así planteada la cuestión, parecería entonces que esa función ordenadora de la vida del hombre en sociedad ha dado lugar a una nueva generación de ámbitos íntimos que, como tales, reclaman algún tipo de protección contra las pulsiones arbitrarias de las agencias encargadas de la persecución y represión del delito.

Obsérvese, al respecto, que con sólo revisar la información contenida en cualquier teléfono de las características señaladas es posible conocer, entre otras cosas, las llamadas que la persona realizó y las que recibió, acceder al contenido de los mensajes de texto y de correo electrónico enviados y recibidos, sus movimientos bancarios (4), archivos de foto y video, como así también escuchar las notas de voz, relevar todos los contactos de la agenda de

(1) Véase la historia completa en el sitio web http://diariodeunteleco.wordpress.com/2007/05/22/martin-cooper-y-la-primera-llamada-desde-un-movil/.

(2) En la actualidad es muy común que los bancos ofrezcan servicios para que los usuarios de celulares puedan consultar los saldos de sus cuentas, realizar transferencias de dinero y visualizar las ya realizadas, pagar servicios e impuestos con tarjeta de crédito, etcétera. Para poder operar el cliente debe instalar un *software* en su equipo y seleccionar un nombre de usuario y contraseña. Véase, en este sentido, el servicio Link Celular que ofrece el Banco de la Ciudad en el sitio web http://www.bancociudad.com.ar/personas/link-celular.

(3) Así, por ejemplo, el Blackberry 8900 Javelin Baby Bold permite escuchar los llantos de un niño que duerme en la cuna.

(4) Nada impediría a la policía husmear libremente el contenido de correo electrónico ajeno si el usuario tuviese por ejemplo instalado y configurado en su teléfono celular algún *software* que cumpliese la función de "administrador de correo electrónico" (*vgr.*, el Outlook Express, elaborado por la firma Microsoft), por cuanto en tal caso ni siquiera será necesario el ingreso previo de clave o contraseña alguna para proceder a su inspección. Se trata, en efecto, de las cuentas de correo del tipo "POP.3", en las que el usuario baja sus archivos de correo directamente al celular, donde quedan almacenadas, las cuales se distinguen de las cuentas "IMAP" (*Interactive Mail Access Protocol*), cuyos archivos permanecen resguardados en un servidor y no en la memoria del teléfono.

direcciones con sus respectivos teléfonos y domicilios, descargar todos los archivos adjuntos, e incluso conocer –con elocuente exactitud– los lugares o locaciones que se hubiesen visitado en caso de que el usuario hubiese activado el sistema de posicionamiento global (GPS).

Por ello trataremos de demostrar que cualquier registro y/o revisación del contenido de un teléfono Blackberry puede llegar a resultar una intromisión ilegítima en la esfera de intimidad de las personas si no se realiza bajo determinadas condiciones señaladas por las normas procesales y constitucionales.

Éste es, en resumidas cuentas, el horizonte de proyección de este breve ensayo, cuyo objetivo no es otro que hacer un humilde y pequeño aporte al siempre candente debate jurídico-constitucional en torno a los límites frente a la averiguación de la verdad, la cual –de modo imperfecto– constituye una de las principales metas del proceso penal, como así también la necesidad de preservar que éste continúe siendo una garantía de libertad del ciudadano **(5)**.

II. ¿LA INFORMACIÓN ALMACENADA EN UN "*SMARTPHONE*" PUEDE CONSIDERARSE COMPRENDIDA DENTRO DEL DERECHO CONSTITUCIONAL A LA INTIMIDAD? LA EXPECTATIVA DE PRIVACIDAD DEL CIUDADANO

No es ocioso recordar que la intimidad o privacidad –en tanto garantía de libertad negativa– ha sido definida como cualquier cosa que uno quiera mantener fuera de la vista de otro, o como el derecho a ser dejado a solas por el Estado.

Este derecho fue reconocido como un baluarte de la dignidad humana, de tal suerte que cualquier intromisión en esta esfera debe ser autorizada por una norma que especifique y justifique en qué casos se permitirá tal injerencia.

Desde antiguo la Corte Suprema de Justicia de la Nación en numerosos pronunciamientos ha venido reafirmando esta idea, más o menos en los siguientes términos: "...sólo por ley podrá justificarse la intromisión [en la vida privada], siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen" **(6)**.

Ahora bien, teniendo en cuenta que nuestro constituyente de 1853 no imaginó los alcances de una revolución en las telecomunicaciones que diera lugar a la existencia de pequeños equipos móviles que almacenan gran cantidad de información, corresponde entonces formular nuestros primeros interrogantes: *¿cabe darle algún tipo de protección a los datos de alta sensibilidad personal usualmente almacenados en estos modernos teléfonos móviles? ¿Pueden tales dispositivos ser considerados nuevos espacios de intimidad, o acaso el constituyente quiso dejar desprotegidos estos casos?*

El planteo, claro está, no es menor, si se tiene presente que los nuevos teléfonos móviles han venido a reemplazar –e incluso a optimizar– las funciones y utilidades de otros objetos que otrora desempeñaban un papel preponderante en aquellas actividades que el hombre, desde siempre, ha deseado realizar fuera de la vista o la mirada de sus congéneres, y por supuesto, del propio Estado.

Por tal motivo, en la actualidad es frecuente que la mayoría de los usuarios de estos teléfonos celulares utilicen claves personales y/o códigos (*passwords*) para bloquear el acceso público a la información allí almacenada, de la misma manera que, en los grandes centros urbanos, los individuos no dejarían abierta la puerta de su casa o morada al salir a trabajar, no estacionarían en la vía pública con el baúl del rodado abierto, no olvidarían una agenda con el detalle de sus ahorros o movimientos bancarios a la vista ni revelarían el álbum de fotos familiares a cualquier desconocido curioso.

En otras palabras, aquello que antes se encontraba resguardado del conocimiento de terceros en el interior de cajones, portafolios, armarios, cofres o baúles cerrados bajo llave o candado, hoy es conservado en minúsculos soportes informáticos de telefonía móvil, que cuentan con la opción de incluir claves o contraseñas, aun cuando éstas no hubiesen sido activadas por el usuario, su mera existencia revela la voluntad de éste de que dicho soporte goce de cierta inmunidad frente a interferencias ajenas.

Por ello, y a riesgo de que nuestro punto de partida pudiese resultar de considerable obviedad, creemos que la expectativa de privacidad que los usuarios razonablemente poseen sobre la información almacenada en las aplicaciones (o *software*) de estos nuevos teléfonos inteligentes no se diferencia siquiera un ápice de la de otros ámbitos que la jurisprudencia ha considerado como parte de la vida íntima de las personas **(7)**, y que, por lo tanto, resultan inviolables y merecedores de tutela contra injerencias abusivas **(8)**.

(5) Ver, Ferrajoli, Luigi, "Derecho y razón. Teoría del galantismo penal", Ed. Trotta, Madrid, 2006, p. 603 y ss.

(6) Fallos 306:1892, "Ponzetti de Balbín, Indalia v. Editorial Atlántida S.A.". A su turno, siguiendo la misma línea de interpretación, la Cámara Nacional de Casación Penal sostuvo que las injerencias a la vida privada son extensibles a las injerencias en la correspondencia y otras comunicaciones interpersonales (cfr. C. Nac. Casación Penal, sala 3ª, "Tellos, Eduardo", del 24/3/1994, LL 1995-B-63).

(7) A modo de ejemplo, ver *in re* "Ayala", sala 4ª, en donde la Cámara del Crimen explicó que un cofre cerrado constituye un "recinto privado que debe recibir la misma protección que el domicilio" (LL 1990-E-543); y más recientemente ver *in re* "Redruello", sala 4ª (JA 2005-II, fasc. 10, del 8/6/2005), y "S. R. y otros s/ infr. ley 24769" (ED 204-190), C. Nac. Penal Económico, sala A, en donde se resolvió que las comunicaciones cursadas vía correo electrónico constituyen correspondencia epistolar, cuya inviolabilidad se encuentra garantizada por la Constitución Nacional. Estos y otros pronunciamientos pueden ser consultados en el libro del profesor Carrió "Garantías constitucionales en el proceso penal", 5ª ed., Ed. Hammurabi, Buenos Aires, 2008, p. 433 y ss.

(8) El criterio o doctrina de la "razonable expectativa de privacidad" ha sido formulada y extensamente desarrollada, como bien explica Carrió, por la Corte Federal de los Estados Unidos en los precedentes "Katz v. United States" (389 *US* 347 –1967–), "California v. Ciraolo" (476 *US* 207 –1986–) y "California v. Greenwood" (486 *US* 35 –1988–). Ver Carrió, "Garantías constitucionales..." cit., p. 438.

En consecuencia, desde esta perspectiva, *nada justificaría que los nuevos teléfonos móviles sean desdeñados en tanto nuevos ámbitos de intimidad del hombre que participan de la misma garantía de inviolabilidad que otros recintos considerados tradicionalmente privados por la doctrina y jurisprudencia*.

En última instancia, subyace el propósito de intentar problematizar, una vez más, la clásica noción de privacidad y concepción de Estado, como así también los cambios que ambos conceptos han experimentado en la modernidad.

III. ¿QUÉ NORMAS CONSTITUCIONALES PERMITEN CONSTRUIR LA INVIOLABILIDAD DE ESTOS NUEVOS ESPACIOS ÍNTIMOS?

Al respecto, no debemos soslayar que el constituyente de 1994 introdujo en el párr. 3 del art. 43 de nuestra Carta Magna una modalidad de amparo específico referido a la utilización indebida de datos personales contenidos en bancos públicos o privados, que la doctrina constitucionalista luego denominó "hábeas data" y cuyo estudio pormenorizado supera los límites de este trabajo **(9)**.

Sin embargo, detrás de esta importante reforma subyace la idea de que nuestra Ley Fundamental debe ser interpretada en forma "dinámica", lo que significa, en pocas palabras, que su texto debe ser adaptado continuamente al contexto temporo-espacial en el que el intérprete pretende aplicar sus cláusulas, so pena de despojarlas de toda operatividad y contenido **(10)**.

Por tal motivo nuestra propuesta consiste en entender que *todo dato almacenado en cualquier teléfono móvil inteligente debe gozar, dentro del proceso penal, de análogo resguardo constitucional que los papeles privados y la correspondencia epistolar* (art. 18, CN).

Una solución adversa, ciertamente, acabaría frustrando la razonable expectativa de privacidad orquestada a partir del rápido y explosivo desarrollo que han experimentado las telecomunicaciones móviles en nuestras sociedades modernas. En efecto, nos parece claro que el modelo de Estado constitucional de Derecho cedería su lugar al Estado policial tanto cuando un mitin de policías pueda husmear libremente nuestros documentos privados como cuando otros funcionarios estatales cuenten con amplias facultades para examinar sin restricciones la información almacenada en estos nuevos aparatos.

Ciertamente, en ambos casos se podrá conocer, comentar e incluso divulgar nuestras actividades, gustos y/o preferencias personales, lo que indudablemente equivale a despojar de toda operatividad y contenido a los resguardos reconocidos en nuestro texto constitucional.

Por ello resulta de vital importancia construir normativamente un "escudo protector" contra tales prácticas interpretando *dinámicamente* los derechos y garantías consagrados en los arts. 18 y 19 de nuestra Constitución Nacional.

Conforme a esta perspectiva, el art. 18 constituye una garantía expresa de inviolabilidad que no debe limitarse únicamente a la "correspondencia y los papeles privados" en sentido literal, sino que posee virtualidad para abarcar otras situaciones; mientras que art. 19 del mismo plexo de base debe proteger a la "privacidad", entendida ésta en un sentido bifronte: por un lado, como el derecho de todo ciudadano a ser dejado a solas por el Estado (libertad negativa), y por el otro, en tanto facultad de éste para configurar con absoluta autonomía un ámbito cerrado a cualquier interferencia ajena (libertad positiva) **(11)**.

Así, ambas cláusulas constitucionales, concebidas en forma dinámica, deberían servir para obligar a los agentes estatales a respetar cualquier ámbito en el que los indivi-

(9) Así, en uso de sus facultades reglamentarias (art. 75, inc. 32), el Congreso de la Nación sancionó la ley 25326 de Hábeas Data (publ. BO del 2/11/2000), que "tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos", ya sea públicos o privados, "destinados a dar informes, *para garantizar el derecho al honor y a la intimidad de las personas* (...), de conformidad a lo establecido en el art. 43, párr. 3, CN". Conforme a lo expuesto, es indudable que la *ratio legis* que inspiró esta modalidad de amparo constitucional ha sido la protección de la privacidad de las personas cuando ella pueda resultar afectada en virtud de la publicación de datos falsos, inexactos y/o desactualizados que deban considerarse "sensibles". Véase, asimismo, que el art. 32 de dicha ley incorporó los arts. 117 bis y 157 bis a la legislación penal, castigando así conductas vinculadas al acceso indebido y/o publicación ilegítima de datos personales contenidos en bancos o archivos, entre muchas otras. En suma, tal y como veremos seguidamente, nada impediría a los tribunales aplicar estas disposiciones a datos sensibles contenidos en cualquier clase de teléfono móvil inteligente.

(10) Sobre el particular, nuestra Corte Suprema de Justicia ha fundamentado esta clase de interpretación en los siguientes términos: "...que no se trata en el caso de desconocer las palabras de la ley, sino de dar preeminencia a su espíritu, a sus fines, al conjunto armónico del ordenamiento jurídico y a los principios fundamentales del derecho. De lo contrario, aplicar la ley se convertiría en una tarea mecánica incompatible con la naturaleza misma del derecho y con la función específica de los magistrados que les exige siempre conjugar los principios contenidos en la ley con los elementos fácticos del caso, pues el consciente desconocimiento de uno u otros no se compadece con la misión de administrar justicia" (Corte Sup., "Saguir y Dib C. s/ autorización", del 6/11/1980).

(11) Ahora bien, si las cláusulas de mención fueren insuficientes para convencer, tampoco debería olvidarse que análogos principios fueron receptados por el derecho internacional de los derechos humanos. Así, por ejemplo, los arts. 12, DUDH, 11, inc. 2, CADH, 17.1, PIDCyP y 10, DADDH –tratados con jerarquía constitucional en virtud del art. 75, inc. 22, CN– protegen a la correspondencia de las injerencias arbitrarias y abusivas. Así, en virtud del principio interpretativo *pro homine*, que obliga a escoger la hermenéutica que más derechos acuerde al hombre, parece posible extender la protección a toda clase de información privada.

duos posean un razonable interés de excluir a terceros, lo que, por las razones ya expuestas, debe predicarse con relación a los contenidos de cualquier teléfono móvil (12).

Por último, tampoco se nos escapa que en el tema aquí analizado no sólo está en juego el derecho a la intimidad y la inviolabilidad de los papeles privados, sino también –aunque en menor medida– la garantía que prohíbe la autoincriminación compulsiva reconocida por nuestra Constitución Nacional, por los tratados internacionales incorporados a nuestra Constitución en el art. 75, inc. 22, y por el derecho interno. Resulta harto evidente que los secuestros e inspecciones de todo teléfono móvil son frecuentemente efectuados con el propósito de obligar a su dueño a proveer información que podría gravitar en su contra, con lo cual también podría llegar a ponerse en serio riesgo el principio *nemo tenetur se ipso acussare* si no mediase control judicial alguno sobre la actividad policial.

Sea como fuere, a través de estas humildes reflexiones se pretende evitar cualquier práctica que acabe despojando de toda operatividad y contenido a los derechos y garantías con relación al tema que aquí nos ocupa. Porque sabido es que un derecho no operativo (o cuyo real y efectivo ejercicio se encuentra, en la práctica, vedado a su titular) equivale tanto como a un "no derecho", el cual queda reducido a una mera declamación de buenas intenciones, situación que claramente ha pretendido evitar la línea de precedentes de nuestro Máximo Tribunal Constitucional.

IV. ¿EL ESTADO ARGENTINO ESTÁ DISPUESTO A RECONOCERLE AL INDIVIDUO SU EXPECTATIVA DE MANTENER BAJO RESERVA EL CONTENIDO DE SU TELÉFONO MÓVIL?

A nuestro modo de ver, *es indudable que el Estado argentino, a través de todas sus normas, expresa y comunica socialmente cierta disposición favorable a reconocerle al ciudadano su interés o expectativa por preservar razonablemente estos nuevos ámbitos, sobre todo, contra cualquier invasión arbitraria por parte de cualquiera de sus agentes y funcionarios.*

Por cierto, esta conclusión, tal y como veremos seguidamente, no sólo puede extraerse de las cláusulas constitucionales que ya hemos reseñado, sino también –y fundamentalmente– de toda la normativa infraconstitucional que existe en la materia (13).

Ello es lógico si se tiene presente que las normas constitucionales son las que, en último análisis, informan al legislador penal cada vez que debe definir qué clase de bienes jurídicos habrán de recibir una tutela de mayor intensidad mediante la sanción de prohibiciones penales (14).

Por ello en el tít. V, cap. III, de nuestro ordenamiento penal sustantivo se reprimen con penas de prisión las diversas formas de violación de secretos (art. 153) (15) y otros atentados contra papeles privados (arts. 154 a 155, CPen.). Figuras que, ciertamente, protegen el ámbito de reserva o intimidad de la correspondencia, cualquiera sea su contenido, e incluso con total independencia de que éste pueda llegar a resultar secreto para su destinatario o titular (16).

Más aún, a raíz de los continuos avances tecnológicos en esta materia, el legislador debió reformar el art. 153, CPen. para no dejar fuera del concepto de "papeles privados" a aquellos que se presentasen en soporte informático.

Obsérvese, pues, que el texto original de dicho precepto reprimía al que "abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza". Sin embargo, tras la sanción de la ley 26388, en junio de 2008, la fórmula legal de este tipo penal sufrió una modificación con el objeto de proteger la correspondencia informática. Concretamente, dicha ley agregó el término "comunicación electrónica", agravando la pena cuando el hecho fuese cometido por un "funcionario público que abusare de sus funciones".

Desde esta perspectiva, al reglamentar la garantía de inviolabilidad de la correspondencia y demás papeles privados, el legislador penal acabó otorgándoles nuevos y amplios alcances a los espacios de privacidad de los ciudadanos, los que, claro está, resultaban claramente insospechados e inimaginables para los constituyentes de 1853.

(12) Con otras palabras, aunque compartiendo un enfoque similar, Carrió ha construido las bases constitucionales de la doctrina de la "la razonable expectativa de privacidad", recurriendo a los arts. 18 ("inviolabilidad del domicilio y la defensa en juicio... de los derechos"), 19 ("acciones privadas de los hombres. exentas de la autoridad de los magistrados") y 33 (garantías no enumeradas) de la Constitución Nacional. Ver Carrió, "Garantías constitucionales..." cit., p. 437.

(13) Repárese, tan sólo a modo de ejemplo, en que la Ley Nacional de Telecomunicaciones (ley 19798) en su art. 18 establece que la correspondencia de telecomunicaciones es inviolable, y que su interceptación sólo procederá a requerimiento de juez competente; idénticos principios surgen de la ley 25520, tal como veremos seguidamente.

(14) Al respecto, el profesor Zaffaroni enseña que "El derecho penal recibe el bien jurídico ya tutelado [de la Constitución y los tratados] y la norma que se deduce del tipo no hace más que anunciar un castigo para ciertas formas particulares y aisladas de lesión al mismo" (cfr. Zaffaroni, Eugenio R., Alagia, Alejandro y Slokar, Alejandro, "Derecho Penal. Parte general", 2ª ed., Ed. Ediar, Buenos Aires, 2002, p. 486).

(15) "Será reprimido con prisión de quince días a seis meses, el que abriere o accediere indebidamente una comunicación electrónica, una carta, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido".

(16) Cfr. C. 3ª Crim. y Corr. La Plata, sala 4ª, 26/19/1992; C. Fed. Cap., 13/3/1942, "Brandi, Pablo A.", JA 1942-II-432, entre tantos otros.

Parecería entonces que en la actualidad, tras la modificación del ilícito contenido en el art. 153, CPen., buena parte de la información contenida en un aparato de telefonía móvil inteligente, más allá de que pueda o no ser obtenida mediante una conexión inalámbrica a internet (*Wi-Fi*), ha recibido idéntica tutela penal que la de los papeles privados, ya sea que la acción punible hubiese sido cometida por un particular o bien por los propios agentes estatales encargados de la persecución de delitos.

Sentado cuanto precede, si bien es cierto que la jurisprudencia no se ha expedido expresamente sobre el caso de los celulares recientemente aparecidos en el mercado, sí lo ha hecho con relación a los datos que comúnmente son almacenados en esta clase de aparatos (vgr., correos electrónicos, mensajes de texto, registros de llamadas, etcétera), asimilando su protección a la de la correspondencia privada (17).

Esta asimilación, por otra parte, se ajusta a las previsiones de la Ley de Inteligencia Nacional, cuyo art. 5 establece que "Las comunicaciones telefónicas, postales, de telégrafos o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, *son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario*" (18) (el destacado es nuestro).

En conclusión, no tenemos dudas de que el Estado argentino, a través de todos estos comunicados normativos, ha demostrado que ciertamente está dispuesto a reconocerle al individuo su expectativa de mantener bajo reserva el contenido de su teléfono móvil, asimilando su protección a la de los papeles privados y correspondencia postal.

V. CONSECUENCIAS DE NUESTRA POSTURA Y SU CONFRONTACIÓN CON LA REGULACIÓN EXISTENTE EN LOS CÓDIGOS PROCESALES DE LA NACIÓN Y DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

Ahora bien, si los datos contenidos en los aparatos de telefonía móvil inteligente gozan, dentro del procedimiento penal, de idéntico resguardo constitucional que los papeles privados y la correspondencia epistolar por existir una razonable expectativa de privacidad de su dueño que el Estado posee interés en proteger, *la primera y elemental conclusión es que, como regla general, solamente los magistrados, en tanto custodios de todos los derechos y garantías –según lo establece la misma Constitución (art. 116)–, son los únicos sujetos procesales que pueden válidamente otorgar autorización para que la agencias estatales (funcionarios de las fuerzas de seguridad o del Ministerio Público Fiscal) ingresen en estos nuevos espacios de intimidad con el fin de obtener cualquier información útil para la averiguación de la verdad.*

Si bien es cierto que, apriorísticamente, la exigencia de "autorización judicial previa" no aparece mencionada de modo expreso en el art. 18, CN, cuando nuestra Corte Suprema tuvo oportunidad de establecer los alcances de la garantía de inviolabilidad del domicilio consideró *que, por imperio constitucional, ningún otro funcionario que no sea un juez puede disponer un registro domiciliario* (19), hermenéutica ésta que debe extenderse a cualquier ámbito privado, y por añadidura, a aquellos que constituyen el objeto del presente ensayo.

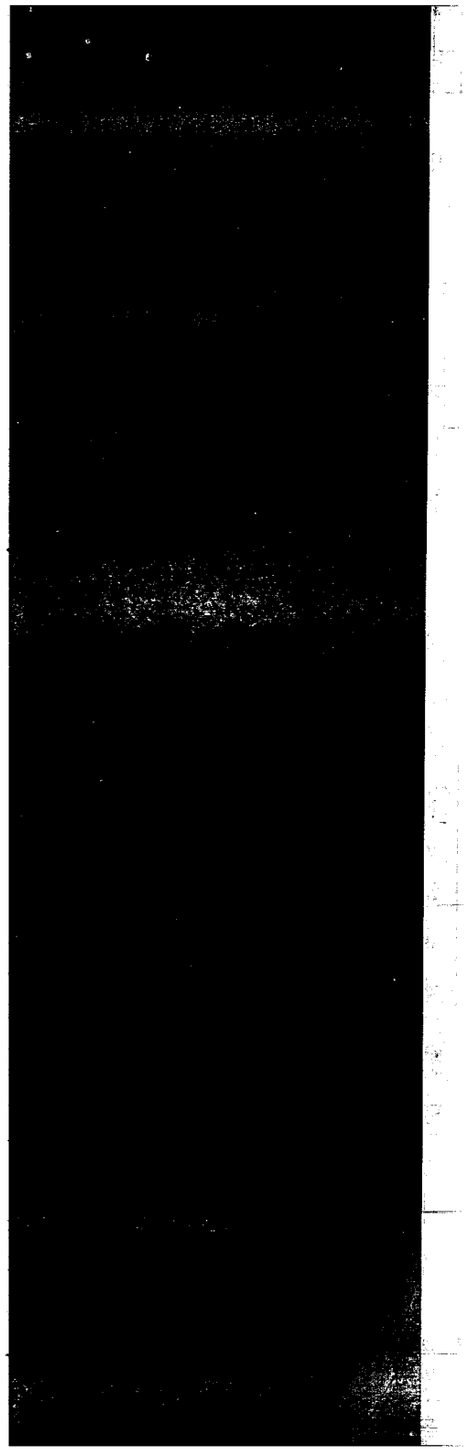
Es que, precisamente, la protección constitucional o garantía de inviolabilidad (art. 18, CN) consiste en que el órgano con mayor imparcialidad y equidistancia dentro del proceso sea el que, mediante el dictado de un auto suficientemente preciso y fundado, examine las "razones justificantes" (20) antes de ordenar cualquier medida que

(17) A modo de ejemplo, la C. Nac. Crim. y Corr. sostuvo que "nada se opone, para definir al medio de la comunicación electrónica como verdadero correo en versión actualizada. La correspondencia y todo lo que por su conducto puede ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los arts. 153 al 155, CPen., cuando no existían avances tecnológicos como el del correo electrónico" (C. Nac. Crim. y Corr. sala 6ª, *in re* "Lanata, Jorge", rta. el 4/3/1999). Más recientemente, la sala 1ª de esa Cámara consideró que "el correo electrónico es correspondencia privada protegida por la Constitución Nacional y otros tratados sobre derechos humanos incorporados a ella, en razón del reconocimiento de la libertad de intimidad y el consecuente derecho a la vida privada, que configuran un valor que está estrechamente relacionado con la dignidad del ser humano en función de la idea política dominante en las sociedades en vísperas del siglo XIX" (C. Nac. Crim. y Corr. sala 4ª, "Redruello, Fabián L.", rta. el 15/11/2004). Por su parte, el TEDH reconoció que se encuentran comprendidos dentro del término "correspondencia" los mensajes de texto (cfr. "Taylor-Sabori v. Reino Unido", sent. del 22/1/2003).

(18) Conf. ley 25520 (publ. BO del 6/12/2001).

(19) Ya en el año 1985 nuestro Alto Tribunal explicaba en "Fiorentino, Diego" lo siguiente: "Aunque en rigor no resulta exigencia del art. 18 que la orden de allanamiento emane de los jueces, el principio es que sólo ellos pueden autorizar la medida..." (Corte Sup., Fallos 306:1752, consid. 5, LL 1985-A-159).

(20) Hemos utilizado la expresión "razones o motivos justificantes" como consecuencia directa de admitir que la protección constitucional de los papeles privados (art. 18, CN) puede válidamente extenderse a los datos almacenados en cualquier teléfono móvil. Así, el art. 18 declara su inviolabilidad y determina que excepcionalmente "una ley determinará en qué casos y con qué *justificativos* podrá procederse a su allanamiento y ocupación" (el destacado es nuestro), siendo que esos "justificativos legales" aparecen regulados en los Códigos Procesales dictados por el Estado Nacional, los Estados provinciales y la Ciudad Autónoma de Buenos Aires. A continuación nos encargaremos de analizar cada uno de ellos.



implique una interferencia en estos nuevos ámbitos de privacidad tributarios de la explosiva revolución en las telecomunicaciones.

No obstante, aun cuando se pretendiese poner en duda esta idea de que sólo los jueces están en mejores condiciones de ecuanimidad (si se los compara con los agentes policiales o con los del Ministerio Público Fiscal) en aquellos sistemas de enjuiciamiento que aún preservan la figura del juez instructor o inquisidor bajo el argumento de que su equidistancia e imparcialidad ha sido enérgicamente cuestionada **(21)**, en cambio, tal fundamento sí es plenamente válida en aquellos modelos procesales regidos por la lógica de la adversarialidad **(22)** (*proceso contencioso inter-partes*), en donde el representante del Ministerio Público Fiscal no pasa de ser una "parte" con una pretensión e interés concreto en el resultado del pleito **(23)**.

Sin perjuicio de ello, véase que aun el propio Código Procesal Penal de la Nación –el cual omitió esa separación entre las funciones de persecución y juzgamiento durante la etapa preparatoria– prohíbe en sus arts. 185 y 234 la apertura de la correspondencia por parte de las fuerzas de seguridad, estableciendo que cualquier interceptación, secuestro y/o examen de la correspondencia postal o telegráfica incautada deberá contar con la intervención fundada de un juez **(24)**. Y si bien este Código permite a los funcionarios policiales, en situaciones de "urgencia", proceder al secuestro de papeles privados sin orden judicial, no es menos cierto que su incorporación dependerá en definitiva de la decisión del juez de la causa, únicamente autorizado para revisar su contenido y decidir su introducción al proceso o debate mediante auto fundado, si entendiese que el mismo resultase útil para la averiguación del hecho que se investiga (cfr. arts. 235 y 356, CPPN) **(25)**.

No obstante, si todavía quedara alguna clase de duda al respecto, cabe recordar que la ley 25760 **(26)** incorporó un párr. 2 al art. 236 de dicho cuerpo de leyes, estableciendo que la obtención de cualquier registro que hubiere de las comunicaciones del imputado o de quienes se comunicaron con él reclama, como condición de validez, la orden previa de un juez competente que disponga la medida manifestando fundadamente la necesidad y objeto de la misma **(27)**.

(21) Para un estudio pormenorizado y exhaustivo de los orígenes históricos y críticas a las tradiciones inquisitivas que posibilitaron aquellos modelos procesales en los que el juez, por iniciativa propia, procede "de oficio" a la búsqueda, recolección y valoración en el ámbito de la prueba, ver Ferrajoli, Luigi, "Derecho y razón..." cit., ps. 563/624.

(22) Tal y como se verá a continuación, el modelo adversarial –en tanto subespecie de los sistemas de enjuiciamiento acusatorios– es el que ha entrado en vigencia el 30/10/2007 mediante la ley 2303 (publ. BOCBA del 8/5/2007), que sancionó el novel Código Procesal Penal para gobernar la Administración de Justicia Penal y Contravencional de la Ciudad Autónoma de Buenos Aires. En efecto, este cuerpo normativo, que entró en vigencia con la pretensión de dejar atrás la aplicación del Código Procesal Penal de la Nación en el ámbito local, en cumplimiento de la manda establecida en los arts. 75, inc. 12, y 129, CN (facultades no delegadas), tuvo por objeto adaptar el sistema de enjuiciamiento criminal a los principios constitucionales propios de la Constitución de la Ciudad Autónoma de Buenos Aires, cuyo art. 13, inc. 3, exigía expresamente el diseño de un procedimiento básicamente acusatorio. De allí que la reflexión que hemos efectuado sobre las facultades de los jueces y fiscales en el tema que aquí nos ocupa tendrá implicancias directas en la interpretación de las disposiciones procesales que rigen la cuestión en el procedimiento penal actualmente vigente en la Justicia porteña.

(23) En efecto, al describir los rasgos característicos de los sistemas acusatorios, Luigi Ferrajoli explica lo siguiente: "La separación de juez y acusación es el más importante de todos los elementos constitutivos del modelo teórico acusatorio, como presupuesto estructural y lógico de todos los demás. Comporta no sólo la diferenciación entre los sujetos que desarrollan funciones de enjuiciamiento y los que tiene atribuidas las de postulación..., *sino también, y sobre todo, el papel de 'parte' –en posición de paridad con la defensa– asignado al órgano de la acusación, con la consiguiente falta de poder alguno sobre la persona del imputado*" (el destacado es nuestro) (Ferrajoli, "Derecho y razón..." cit., p. 567).

(24) Nótese, pues, que la expresión de los fundamentos tiene directa relación con la posibilidad de controlar la decisión (esto es, su necesidad, proporcionalidad, etc.), y por lo mismo, con el adecuado y eficaz ejercicio de toda la actividad recursiva puesta en manos del imputado por imperio del art. 8.2.h, CADH (Pacto de San José de Costa Rica) y demás instrumentos internacionales de rango constitucional.

(25) Siguiendo esta línea interpretativa, la Suprema Corte de Justicia de Mendoza sostuvo que las cartas privadas que había secuestrado la policía sólo podían haber sido leídas por el juez de la causa y no por funcionarios policiales, invocando de esta manera la inviolabilidad de la correspondencia como elemento fundamental "de la libertad de intimidad o del derecho a la privacidad" (*in re* "Pierro", JA 1992-I-443).

(26) Publ. BO del 11/8/2003. Se trata de la muy cuestionada legislación, popularmente conocida como "Antisecuestros", cuya sanción fue orquestada en buena medida por la presión de ciertos sectores sociales y cuyo programa normativo consistió en la introducción de cambios sustanciales en varias normas procesales del Código adjetivo nacional.

(27) Tras esta importante y tan cuestionada reforma (en virtud de haber sido orquestada por presiones de numerosos sectores) al Código Procesal Penal de la Nación, el art. 236 quedó dividido en tres párrafos: el primero, referido a las intervenciones telefónicas en sentido estricto, el segundo, a los requerimientos de llamados entrantes y salientes, y, por último, el tercero otorgó la posibilidad excepcional a los agentes fiscales para intervenir comunicaciones cuando se investigasen los delitos de secuestro extorsivo y privación ilegal de la libertad. Sin embargo, aun en este último supuesto, como acertadamente explica Carbone, la norma no elimina la orden judicial sino que la pospone, de modo que si el juez no la confirma *ex post* (sea porque no se cumplió con el requisito de adecuada fundamentación, proporcionalidad, etc), se fulmina la eficacia de todo lo actuado por el fiscal (Carbone, Carlos, "La ley 25760 y la intervención de las comunicaciones telefónicas por mandato fiscal en el Código Procesal Penal de la Nación" JA del 5/1/2005, ps. 19/25).

Justo es recordar que con anterioridad a la reforma introducida por esta ley no existía en el ámbito nacional protección alguna de los registros de tráfico de las comunicaciones telefónicas, por lo que la policía, los fiscales e incluso los propios jueces accedían a ellas sin límite alguno.

Sin embargo, en la actualidad la praxis forense tampoco pareciera haber asimilado suficientemente el verdadero espíritu y alcance de los cambios normativos apuntados. Es que, en rigor, resulta francamente lamentable que, a pesar de la modificación introducida al art. 236, CPPN, la mayoría de los operadores del sistema penal continúen accediendo indiscriminadamente a los registros de "llamadas entrantes y salientes" de celulares sin sujeción a restricción legal alguna **(28)**, y, lo que es peor, malogrando en muchos casos la actividad recursiva del imputado al no dar a conocer los motivos de hecho y de derecho que determinaron la necesidad de adoptar un medida de tal naturaleza **(29)**.

Esto mismo puede predicarse en el ámbito de la Justicia Penal y Contravencional de la Ciudad Autónoma de Buenos Aires, aun cuando en nuestro medio local la reglamentación legislativa del derecho a la intimidad de ciertos datos y la garantía de inviolabilidad de los mismos (arts. 18 y 19, CN) reconozca una protección, a nuestro juicio, bastante más amplia que la consagrada en el art. 236, CPPN **(30)**.

En efecto, el art. 90, CPP de la Ciudad ha optado por utilizar una fórmula legal que contiene, según creemos, una prohibición mucho más específica con relación al tema de este ensayo, ya que la misma se encuentra dirigida contra cualquier práctica estatal que tenga por objeto la inspección de "datos privados contenidos en soporte informático" **(31)**, expresión ésta que no sólo veda el acceso indebido a los registros de llamadas entrantes y salientes de un teléfono móvil sino a cualquier otro dato que aparezca formando parte del ámbito de reserva del imputado o sobre el cual éste tuviese una razonable expectativa de privacidad.

Es que, a decir verdad, los términos "datos privados contenidos en soporte informático" son tan amplios, que no cabría privar de dicha protección a cualquier información privada o sensible que pudiere encontrarse almacenada en el *software* de un equipo de telefonía móvil, como ser no ya únicamente el registro de llamadas entrantes y salientes, sino también los mensajes de texto, las grabaciones de voz, los archivos de imágenes y sonidos (música, fotografías, etcétera), los datos de la agenda electrónica o libreta de notas, los referentes al sistema de posicionamiento global (GPS), así como toda aquella información que el usuario del aparato opere por vía de alguna conexión inalámbrica a internet (datos de cuentas bancarias, por ejemplo).

Ahora bien, hemos dicho que la prohibición contenida en el art. 90, CPPCABA bajo análisis resulta más amplia y específica que su par de la legislación nacional (arts. 185, 234 y 236, CPPN), por cuanto aquella norma establece que el juez –aun en los *casos de urgencia*– es el único habilitado para decidir mediante auto fundado si corresponde o no acceder a los datos resguardados en el *software* de tales aparatos, otorgándole, una vez que hubiese revisado su contenido, la facultad de delegar en las fuerzas de seguridad cualquier diligencia pericial que deba prac-

En similar sentido, puede consultarse la opinión de Luis García en su artículo "La vigilancia de las telecomunicaciones y otras comunicaciones interpersonales según la jurisprudencia elaborada en torno al Código Procesal Penal de la Nación", publicado en el libro "Garantías constitucionales en la investigación penal. Un estudio crítico de la jurisprudencia", Plazas, Florencia G. y Hazan, Luciano A. (comps.), Ed. del Puerto, Buenos Aires, 2006, p. 313 y ss.

(28) En efecto, no son muchos –ni frecuentes– los pronunciamientos de los tribunales nacionales de alzada decretando la nulidad de cualquier diligencia tendiente a obtener los listados de llamadas entrantes y salientes en infracción al requisito de judicialidad de la medida. Recientemente, sin embargo, la sala 7ª de la Cámara Criminal y Correccional de la Capital Federal ha efectuado un prolijo análisis de la cuestión. En el caso el fiscal de la causa había ordenado mediante un simple decreto –esto es, sin expresar motivación alguna– a la firma Telecom Personal S.A. el listado de las llamadas entrantes y salientes del imputado. Ahora bien, aun cuando no formara parte de los agravios de la defensa, la Cámara resolvió declarar "de oficio" la nulidad de la medida considerando que la misma resultaba resorte exclusivo del juez de la causa, mientras que el Ministerio Público Fiscal únicamente podría hacerlo, a tenor del párr. 3 del art. 236, CPPN, cuando estuviese involucrada alguna de las figuras penales contenidas en los arts. 142 bis y 170, CPPN, se verificara un peligro en la demora y la diligencia se encontrase debidamente justificada (causa 36.280, "S., R. s/ procesamiento, abuso sexual", rta. el 27/3/2009). Ver, con un criterio similar al expuesto, C. Nac. Casación Penal, sala 3ª, *in re* "Mitchell, Alejandro", rta. el 4/9/2007.

(29) "La exigencia de fundamentación sirve no sólo a la publicidad y control republicanos, sino también persigue la exclusión de decisiones irregulares o arbitrarias, y poner límite a la libre discrecionalidad del juez, posibilitando el control de sus decisiones" (cfr. García, Luis, "La vigilancia de las telecomunicaciones..." cit., ps. 313 y 327).

(30) Tales prácticas también son, en efecto, bastante frecuentes en la investigación y juzgamiento de las conductas reprimidas por el Código Contravencional de la CABA (ley 1472), razón por la cual las consideraciones que siguen son, a nuestro entender, perfectamente válidas en ese ámbito del derecho por imperio del art. 6, Ley de Procedimientos 12, que ante una laguna normativa obliga al intérprete a aplicar supletoriamente las disposiciones del CPPCABA al procedimiento contravencional.

(31) El art. 90, CPPCABA reza lo siguiente: "*Prohibición de abrir correspondencia o inspeccionar datos privados*. Los integrantes de la policía y otras fuerza de seguridad no podrán abrir la correspondencia que secuestren, ni inspeccionar *datos privados contenidos en soporte informático*, sino que la remitirán a la autoridad judicial o del Ministerio Público Fiscal competente; sin embargo, en los casos urgentes, podrán ocurrir al juez competente más cercano, la que autorizará la apertura de considerarlo oportuno. Una vez conocido el contenido, el/la juez/a podrá autorizar a los integrantes de fuerzas de seguridad la inspección de correspondencia y datos privados contenidos en soporte informático legalmente incautados, a los fines periciales" (el resaltado nos pertenece).

ticarse sobre ellos, fijándole límites bien precisos para evitar que la medida acabe transformándose en abusiva.

En conclusión, sólo los magistrados del Poder Judicial de la Ciudad Autónoma de Buenos Aires poseen, conforme a la ley procesal penal local, facultades para "autorizar la apertura de considerarlo oportuno" (art. 90), esto es, evaluando previamente la necesidad y razonabilidad de proceder a la revisión de los datos almacenados en el soporte informático (o software*) de cualquier teléfono celular, sin perjuicio de la posibilidad de los fiscales de ordenar su secuestro y debido resguardo hasta tanto se obtenga la venia del juez de garantías para proceder al examen de su contenido.*

Las razones que dan sustento a esta hermenéutica se deducen con facilidad no sólo del alcance que les hemos conferido a las cláusulas constitucionales ya mencionadas sino, fundamentalmente, de la reglamentación legal que de ellas se ha hecho para el proceso penal que rige en el ámbito de la Ciudad Autónoma de Buenos Aires. A nuestro entender, tal actividad reglamentaria resulta razonable (art. 28, CN), y es posible conocerla mediante una lectura sistemática y literal de los arts. 90, 93, parte final y 42, CPPCABA.

Nótese, en primer lugar, que el art. 90 –cuyo título reza "Prohibición de abrir correspondencia o inspeccionar datos privados"– *ordena a las fuerzas de seguridad a "remitir intacto" –sic–* el soporte informático incautado al juez o al agente fiscal más próximo. *No obstante, cuando la misma norma escoge a la autoridad encargada de autorizar su revisión parece claro haberse inclinado expresamente por la del "juez competente", no así por la de los órganos estatales encargados de la persecución y sanción del delito* **(32)**.

Aquí, pues, resulta de plena aplicación la vieja regla o máxima interpretativa *ubi lex, sed lex*, que autoriza al intérprete a distinguir situaciones solamente cuando el mismo texto legal lo hiciese **(33)**, no permitiendo el aludido art. 90 realizar al respecto distingo alguno, por cuanto confiere la potestad precitada a los jueces en forma exclusiva y excluyente.

Por otra parte, esta misma télesis parece desprenderse del juego armónico existente entre las restricciones procesales establecidas a la actividad investigativa del Ministerio Público Fiscal de la CABA en el tít. II, cap. 2, del digesto adjetivo local (art. 93, *in fine*) **(34)** y aquellas vinculadas a los aspectos formales que deben observar los decisiones del proceso, cuyo art. 42, inc. 2, anteúltimo párrafo, dispone que toda medida que limite o restrinja derechos o garantías constitucionales del imputado –entre ellas, aquellas que impliquen un ingreso a su ámbito de intimidad o libertad negativa– sólo podrá ser adoptada por el juez de garantías mediante auto motivado, bajo consecuencia de nulidad **(35)**.

En conclusión, dentro de nuestro sistema procesal local, de claros contornos acusatorios, las fuerzas de seguridad y la parte acusadora en ningún caso podrían prescindir de la autorización previa del juez de garantías para proceder a la inspección de cualquier dato contenido en un teléfono móvil, partiendo de la premisa de que su dueño posee sobre éste una razonable expectativa de privacidad constitucionalmente resguardada por el propio Estado (arts. 18 y 19, CN), y cuya intromisión por parte de cualquiera de sus agencias de investigación y persecución penal se encuentra expresamente sancionada con la nulidad (arg. art. 42, inc. 2 y anteúltimo párrafo, y 71, párr. 2, CPPCABA) **(36)**.

(32) Por tal motivo, el art. 90, CPPCABA expresa que "las fuerzas de seguridad (...) la remitirán a la autoridad judicial o del Ministerio Público Fiscal competente; *sin embargo, en los casos urgentes, podrán ocurrir al juez competente más cercano, el que le autorizará a la apertura de considerarlo oportuno(...)*" (el destacado es nuestro).

(33) En su formulación latina, este principio reza: *ubi lex non distinguit, nec non distinguere debemus* (donde la ley no distingue, nosotros no debemos distinguir). Entre otras cosas, este aforismo impedía a los jurisconsultos del derecho romano clásico efectuar distinciones interpretativas sin sustento en el propio texto legal. Vale decir, las diferenciaciones hermenéuticas eran válidas en tanto el legislador las hubiese plasmado expresamente en el texto normativo en cuestión. Sin embargo, el art. 90, CPPCABA no efectúa distinción alguna en cuanto a las posibilidades del fiscal para inspeccionar la información privada contenida en cualquier soporte informático. Por el contrario, la norma otorga dicha facultad, en forma exclusiva y excluyente, a los magistrados.

(34) Art. 93, CPPCABA: "*Actos de Investigación*. A fin de desarrollar la investigación preparatoria el/la fiscal (...). *Deberá solicitar orden judicial para practicar allanamientos, requisas o interceptaciones de comunicaciones o correspondencia*" (el destacado es nuestro).

(35) Art. 42, CPPCABA: "*Resoluciones. Motivación*. Las decisiones de los/las jueces/as se expresarán mediante: ...2) auto, para resolver un incidente o artículo del proceso, para disponer alguna medida que limite o restrinja garantías constitucionales. Las sentencias, autos y decretos serán firmados y los dos primeros motivados, bajo consecuencia de nulidad...".

(36) Una interpretación similar a la aquí desarrollada aunque referida no ya a la información almacenada dentro de los soportes informáticos de los aparatos de telefonía móvil, sino a los casos de intervención de telecomunicaciones u obtención de los registros de tráfico de comunicaciones telefónicas, se encuentra muy bien desarrollada por Luis M. García. En efecto, según este autor, cualquier actividad investigativa que implique alguna injerencia en esos ámbitos se encuentra reservada exclusivamente a la decisión de los jueces, según la interpretación conjunta de los arts. 212, 213 y 236, CPPN. Así también, sostiene que, en líneas generales, tales facultades no han sido igualmente conferidas a los fiscales, quienes no las pueden disponer por sí mismos, poniendo como ejemplo los arts. 329 y 138, CPP de la provincia de Chubut, que vedan expresamente a los fiscales a cargo de la investigación penal preparatoria tal clase de potestad, salvo en los supuestos de peligro en la demora, en cuyo caso la medida quedará sujeta a ratificación por el juez dentro del tercer día (cfr. García, Luis M., "La vigilancia..." cit., p. 324, nota 85).

Obsérvese, empero, que el claro sentido prohibitivo que surge del juego de las cláusulas procesales analizadas (arts. 90, 93, *in fine*, y 42, inc. 2, CPPCABA) podría considerarse reñido con los términos de los arts. 115 y 116 del mismo Código de rito, los cuales parecerían autorizar, *en casos urgentes*, a los representantes del Ministerio Público Fiscal a acceder a cierta información privada sin contar previamente con la orden judicial respectiva **(37)**.

Desde este ángulo, los arts. 90, 115 y 116, CPPCABA parecerían incurrir en graves contradicciones. Ello así, por cuanto el art. 90 dispone que la apertura o examen del material incautado, aun en casos de urgencia, sólo procederá cuando el juez lo ordene; y a la par, los arts. 115 y 116 establecen que el fiscal, en iguales hipótesis urgentes, podrá prescindir de la orden judicial y disponer su apertura bajo su exclusiva responsabilidad.

De allí que no sería ilógico que el lector se preguntase lo siguiente: en definitiva, *¿puede o no la Fiscalía en casos urgentes obviar la autorización judicial previa para revisar la información almacenada en el material informático incautado?*

La respuesta no es tan simple, porque ineludiblemente la legislación procesal local distingue varias situaciones en este tópico.

No obstante, creemos que la inconsistencia puede superarse –atendiendo a la naturaleza "excepcional" de la medida en estudio– si se interpretan los arts. 115 y 116 en sentido literal, o, lo que es lo mismo, entendiendo que sendos dispositivos habilitan a los fiscales a revisar la información contenida en la "correspondencia escrita u otro objeto enviado o recibido vía postal", y siempre que se acreditare algún fundado supuesto de "urgencia" **(38)**, no pudiéndoselo hacer en ningún otro caso **(39)**.

Por otro lado, a idéntica conclusión puede arribarse si se repara en que los términos utilizados en los arts. 115 y 116, CPPCABA han sido copiados textualmente, aunque con algunas modificaciones (propias del modelo acusatorio vigente en la Justicia de la Ciudad), de los consignados en los arts. 234 y 235, CPPN, preceptos éstos que, desde antiguo, autorizada doctrina consideró exclusivamente referidos a cualquier clase de "escrito, documento, valor, pliego o paquete remitido por cualquier vía, sea al imputado por un tercero o por aquél a éste" **(40)**. En definitiva, limitados específicamente a la interceptación de correspondencia postal, telegráfica y/o cualquier paquete postal **(41)**.

Por lo tanto, la respuesta al interrogante que formuláramos anteriormente puede sintetizarse del siguiente modo, a saber: *no corresponde que la parte acusadora invoque cualquiera de los preceptos aquí analizados (arts. 115 y 116, CPPCABA) en ausencia de situaciones de urgencia y/o cuando pretendiese inspeccionar por sí misma cualquier dato privado contenido en el soporte informático (o* software*) de un teléfono móvil, supuestos éstos en los que inextricablemente la vindicta pública deberá requerir la autorización judicial previa por imperio de los arts. 90, 93, in fine*, y 42, inc. 2, CPPCABA.

(37) Así, el art 115, CPPCABA reza lo siguiente: "*Interceptación de correspondencia. Prohibición. Urgencia*. Siempre que lo considere útil para la comprobación del hecho, ante el pedido fundamentado del/la fiscal, el/la juez/a ordenará, mediante auto, la interceptación y el secuestro de la correspondencia postal o telegráfica o de todo otro efecto remitido por el/la imputado/a o destinado a éste en cualquier soporte, aun cuando sea bajo nombre supuesto. *Los integrantes de la policía y fuerzas de seguridad deberán remitir intacta la correspondencia secuestrada a la autoridad judicial o del Ministerio Público Fiscal competente. En los casos urgentes, podrán ocurrir a la más inmediata, la que autorizará la apertura si lo creyere oportuno*" (el destacado es nuestro).
Por su parte, el art. 116 establece lo siguiente: "*Apertura y lectura*. Recibida la correspondencia o los efectos interceptados, el/la fiscal procederá a su apertura en presencia del secretario, dejando constancia en acta. Deberá examinar los objetos y leer por sí el contenido de la correspondencia. Si tuvieren relación con el proceso ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá de la entrega al destinatario, a sus representantes o parientes próximos, bajo constancia. *En el examen de la correspondencia o el resultado de la interceptación de comunicaciones se hará bajo responsabilidad del/la fiscal que lo solicitó*" (el destacado es nuestro).

(38) A nuestro modo de ver, la razón de ello se desprende del texto mismo del art. 115, CPPCABA. Ello, en tanto el párr. 1 de esa norma se refiere a "...la correspondencia postal o telegráfica o de todo otro efecto remitido por el imputado o destinado éste en cualquier soporte", mientras que el párr. 2, por el contrario, se ciñe a la "correspondencia secuestrada", autorizando a la acusación a proceder a su apertura si –mediando urgencia– lo creyere oportuno. Sin embargo, también aquí resulta difícil imaginar cuáles serían esos "casos urgentes" que impidiesen al agente fiscal aguardar la venia del juez antes de proceder a su apertura, máxime cuando el objeto secuestrado ya hubiese sido remitido a la sede de la Fiscalía y se encontrare en su poder.

(39) Nótese, siguiendo esa línea, que los aludidos arts. 115 y 116 se encuentran ubicados bajo el cap. 3, titulado "Intervención de comunicaciones", y cuyos términos gramaticales sólo poseen sentido en tanto se los vincule a la correspondencia escrita, telegráfica o cualquier efecto remitido o recibido por el imputado a través de una encomienda u otro modo análogo de envío o recepción postal.

(40) Ésta es la opinión de Ricardo Núñez, citada por Francisco J. D'Albora en su "Código Procesal Penal de la Nación. Anotado, comentado, concordado" t. I, 7ª ed., Ed. LexisNexis, Buenos Aires, 2005, p. 512 y ss. Comparte esta postura José I. Cafferata Nores en su libro "La prueba en el proceso penal. Con especial referencia a los Códigos Procesales Penales de la Nación y de la Provincia de Córdoba", 6ª ed., Ed. LexisNexis, Buenos Aires, 2008, p. 261.

(41) Es interesante traer aquí a colación un fallo en el que la sala 2ª del Tribunal Supremo español adoptó una interpretación amplia de la noción de correspondencia a efectos de extender las gárantías constitucionales de inviolabilidad a los "paquetes postales". En ese sentido, explicó que "en un paquete postal se pueden incluir objetos que excediendo del volumen de lo que es una carta o misiva tengan un connotación personalísima o íntima que no puede ser investigada si no es con la previa autorización judicial" (TSE, sala 2ª, 25/6/1993, 23/12/1994 y 3/6/2002, LL España, n. 5617, del 23/9/2002).

Asimismo, no debe olvidarse que durante el trámite legislativo del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires la totalidad de los despachos elaborados por las Comisiones de la Legislatura porteña fueron contestes en sostener que "la orden de allanamiento, intervención de comunicaciones y correspondencia deben provenir *exclusivamente* del juez competente" **(42)** (el destacado es nuestro).

Es claro, entonces, que los legisladores, con buen y saludable criterio, realizaron su labor reglamentaria bajo el entendimiento de que dentro de cualquier sistema acusatorio-adversarial los funcionarios del Ministerio Público Fiscal revistan la calidad de "parte", y por tanto no poseen la misma equidistancia o ecuanimidad que los magistrados para evaluar la adopción de cualquier medida intrusiva que afecte estos nuevos ámbitos de la vida íntima. Consiguientemente, *toda invasión de la esfera privada del imputado que no hubiere recibido la autorización previa del magistrado conllevará expresamente la sanción de nulidad* (arts. 42, inc. 2, y 71 y ss., CPPCABA), a excepción, claro ésta, de las situaciones de urgencia que se verifiquen con relación a la correspondencia escrita (postal o telegráfica).

Por otro lado, a nuestro entender, el digesto de rito local ha establecido una protección más rigurosa para el examen de los *"datos contenidos en soportes informáticos" (art. 90) que el que pretenda practicarse sobre la vía postal o telegráfica (arts. 115 y 116)* **(43)**, por cuanto en el primer caso la expectativa de privacidad del ciudadano es más acentuada que en el segundo, ya que "para su funcionamiento se requiere un prestador del servicio, el nombre de un usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse" **(44)**.

En síntesis, el esquema interpretativo que aquí proponemos es, a nuestro ver, el que mejor se compadece con la naturaleza restrictiva que surge del respeto por las garantías constitucionales involucradas, y sobre todo, con el alcance asignado a ellas por nuestro Código Procesal Penal local.

Sin embargo, debemos reconocer que tanto en el ordenamiento procesal local como en el nacional existe un importante número de cuestiones que aún no han sido exhaustivamente reguladas y que resultan de vital importancia para circunscribir el poder discrecional de los jueces al momento de evaluar la aplicación de cualquier medida intrusiva en estos nuevos ámbitos privados.

Es que cuando el poder constituyente estableció que la ley reglamentaria determinará en qué casos y bajo qué justificativos podrá autorizarse la injerencia (art. 18, CN), delegó en los Estados provinciales la facultad para reglamentar tales tópicos en sus respectivos Códigos Procesales, los cuales, en la práctica, no precisaron suficientemente los "casos" y "justificativos", ni el modo en que los datos obtenidos deben ser resguardados, ni el destino que debe darse a aquellos que no tuvieren relación alguna con el objeto de la medida **(45)**.

Como estricta derivación de lo anterior, los ordenamientos procesales (nacional y local) han olvidado fijar parámetros claros y concretos que deban verificarse antes de disponer judicialmente una medida de esta índole, lo que obligará a la jurisdicción a definir si basta con la existencia de una "simple sospecha" o si, en cambio, la ley de rito reclama un estándar más exigente, tal y como sucede con los institutos de requisa, allanamiento y/o detención de personas **(46)**.

Por lo pronto, y sin intenciones de agotar aquí esta problemática, creemos que debe ponerse coto a la libertad de apreciación de los jueces **(47)**, para lo cual habrá que tener en cuenta que el estándar que, en definitiva, se adopte debería ser compatible con la naturaleza "excepcional" de la medida **(48)**. Sólo así resulta plausible restringir al máximo las posibilidades del juez para disponer la intromisión en la información privada contenida en estos nuevos y tecnológicos celulares **(49)**.

(42) Ver Debate Parlamentario, 5ª sesión ordinaria de la Legislatura del 29/3/2007, VT-7, ps. 30, 99 y 99, en particular, el despacho 1245 elaborado por la Comisión de Justicia.

(43) Recuérdese que, tratándose de datos informáticos, sólo el juez puede autorizar la injerencia aun en casos de urgencia, no así en los casos de correspondencia postal o telegráfica.

(44) Cfr. C. Nac. Crim. y Corr., sala 6ª, "Lanata, Jorge s/ desestimación", rta. el 4/3/1990.

(45) A modo de ejemplo, la ordenanza procesal alemana establece que la información obtenida a partir de una intervención telefónica que no posea vinculación con la base del juicio debe ser inmediatamente destruida bajo el control de la Fiscalía, tan pronto como ya no sea necesaria para la persecución penal, o bien en caso de sobreseimiento o de condena firme (parágs. 100.a y 100.b, VI) (cfr. Roxin, Claus, "Derecho Procesal Penal", Ed. del Puerto, Buenos Aires, 2000, p. 305). A propósito de ello, justo es señalar que el legislador porteño se ha limitado a regular algunas de estas cuestiones solamente con relación a la correspondencia postal o telegráfica (conf. art. 116, párr. 2), pero olvidó hacerlo para los datos privados contenidos en soporte informático (art. 90) y aquellos que se hubieran conocido de resultas de la interceptación de una comunicación telefónica.

(46) Por ejemplo, ante esta laguna normativa, la sala 3ª de la C. Nac. Casación Penal en "Mitchel, A.", rta. el 4/9/2007, debió crear pretorianamente un estándar propio sin base legal. En el fallo estableció que el juez debe verificar la existencia de "elementos objetivos y suficientes que determinen la necesidad de adoptarla", lo que, claro está, parecería superar ampliamente la simple sospecha de comisión de un ilícito. Sin embargo, nos parece que esta cuestión debió haberse regulado con mayor profundidad, porque "la oportunidad y/o utilidad de la medida" para la comprobación del hecho (conf. arts. 90 y 115, CPPCABA) abren la puerta al decisionismo y a la arbitrariedad de los magistrados.

(47) Si bien en materia penal rige la libertad o amplitud de valoración probatoria, no hay que olvidar que la "sana crítica racional" impone ciertas limitaciones al juzgador a la hora de apreciar los elementos de juicio con anterioridad a efectuar cualquier operación lógico-inductiva en el ámbito de la prueba que hubiese sido colectada.

Así las cosas, y a título de ejemplo, no debería poder accederse a los mensajes de texto, correos electrónicos o de voz y/o listado de llamados entrantes y salientes si el hecho investigado no tiene siquiera apariencia de ilicitud (o relevancia jurídico-penal), así como tampoco si a partir del indicio ofrecido por la acusación no cabe conjeturar inductivamente –con arreglo a la sana crítica racional o a las máximas de la lógica y la experiencia– ilicitud alguna, o bien si ésta no tuviese relación con los motivos o razones previas utilizadas para fundar la solicitud de la injerencia estatal (vgr., no podría el juez autorizar el acceso a aquellos mensajes de texto que no estuvieran vinculados directamente con las sospechas previas que hubieren alegado la Fiscalía o las fuerzas de seguridad) **(50)**.

Por idénticas razones, ningún juez debería habilitar la intrusión si los antecedentes ofrecidos por la acusación fuesen *frágiles* por su vaguedad, ambigüedad o por haber sido obtenidos de fuentes anónimas **(51)**. Tampoco correspondería la intromisión cuando la medida no fuese proporcional al presunto delito investigado **(52)**.

Así también, creemos que le es exigible al juzgador el intento de limitar al máximo la inspección de estos ámbitos siempre que le fuese posible, circunscribiendo los mensajes de texto o los correos de voz cuya revisión va a autorizar indicando sus fechas y horarios, a efectos de evitar que la orden judicial se acabe transformando en un "cheque en blanco" para que la policía ejecute la medida sobre todo el contenido del aparato **(53)**.

Con todo, las pautas hasta aquí esbozadas son, a nuestro modo de ver, limitaciones concretas cuya observancia corresponde exigir a la actividad decisoria de los jueces, ya que el Estado de Derecho se resiente en igual medida tanto cuando los abusos provienen de las agencias policiales como cuando los jueces poseen facultades irrestrictas sobre la vida privada de las personas.

VI. CONCLUSIONES: LA REGLA DE EXCLUSIÓN DE PRUEBA ILÍCITA

Sobre la base de todo lo expuesto, podemos afirmar que sólo el juez, por imperativo constitucional, se encuentra habilitado para disponer medidas de estas características, y, en consecuencia, ningún otro funcionario puede ordenarlas, y menos aún llevarlas a cabo por iniciativa propia.

De esta manera, las fuerzas de seguridad o el órgano de persecución no pueden inspeccionar los contenidos de un aparato de telefonía móvil inteligente sin una orden judicial previa y suficientemente fundada.

En consecuencia, salvo que mediaren razones de urgencia (arts. 235, CPPN y 115, CPPCABA), cuando la policía o los fiscales revisen por propia iniciativa un teléfono móvil sin esa orden judicial, los elementos de prueba así obtenidos deberán ser reputados ilegales, y por aplicación de

(48) Así, cuanto menos, viene impuesta por la parte 2ª del art. 18, CN, que dispone que, a modo de excepción, "una ley determinará con qué justificativos podrá procederse a su allanamiento y ocupación". Este recaudo de excepcionalidad también se vislumbra en los propios preceptos procesales que regulan la cuestión (art. 236, CPPN, etc.).

(49) Así, siguiendo la opinión del profesor Roxin, el juzgador debería verificar, como primer paso, la existencia de circunstancias o indicios que permitan fundar la sospecha de que el sujeto ha cometido, en calidad de autor o partícipe, un hecho punible, parámetro éste que permite desechar por insuficientes las meras suposiciones o conjeturas (cfr. Roxin, Claus, "Derecho Procesal Penal" cit., p. 306) Recordemos, pues, que un "indicio" es una circunstancia fáctica conocida y probada que, teniendo relación con el hecho investigado, autoriza, por vía de inducción, a concluir sobre la existencia de otras circunstancias fácticas relevantes (el art. 239, Código de Processo Penal brasilero dice: "*Considera-se indício a circunstancia conhecida e provada, que, teniendo relação com o fato, autorize, por indução, concluir-se a existencia de outra ou outras circunstâncias*").

(50) Por ejemplo, si la Fiscalía investiga algún tipo de fraude u otro delito económico, es lógico que la inspección del aparato deberá ceñirse exclusivamente a las aplicaciones en donde consten los movimientos bancarios efectuados por el imputado. No correspondería, por tanto, que la medida permitiese revelar información sobre los gustos musicales, sitios web visitados, etcétera.

(51) Esto es lo que sucedería si, por ejemplo, los agentes prevencionales o la vindicta pública ofreciesen como *notitia criminis* el relato proveniente de una llamada anónima o de un "ocasional transeúnte" cuya identidad, sin explicación alguna, no fue suficientemente individualizada y cuya versión de cargo, en definitiva, tampoco describiese con precisión actividad delictiva alguna. En tales casos, a nuestro ver, si bien tales antecedentes podrían llegar a dar lugar a "meras o simples sospechas", entendemos que no deberían resultar lo suficientemente poderosos como para que el juzgador autorice la injerencia en estos ámbitos. Con todo, no cualquier episodio o indicio conocido por los encargados de ejercer la persecución estatal debería dar lugar a la revisión del contenido de un teléfono de última generación.

(52) Aquí deberíamos preguntarnos seriamente si el juez podría autorizar una invasión de esta gravedad con el objeto de comprobar la comisión de una presunta contravención reprimida exclusivamente con pena de multa. A nuestro juicio, la respuesta a este interrogante no es tan sencilla ni obvia.

(53) A fin de lograr tal cometido debería dársele suficientes posibilidades a la defensa de presenciar el acto de peritaje o desgrabación (correo de voz), o bien, la oportunidad de ofrecer un perito que controle que la medida se ejecute cumpliendo los límites judicialmente impuestos. Ahora bien, cuando se hubiese decretado el secreto de las actuaciones, y por tanto la defensa no pudiese ejercer dicho control, a nuestro ver, nada impediría que el magistrado exigiese a los órganos encargados de ejecutar la medida que lo hicieren en presencia de dos testigos civiles para que controlen el estricto cumplimiento de las limitaciones impuestas a la inspección del aparato.

la doctrina de la *exclutionary rule*, su utilización dentro del proceso estará vedada, aun cuando los elementos incriminantes extraídos del aparato resultasen útiles para el esclarecimiento del hecho delictuoso investigado **(54)**.

Es que de convalidarse el registro de un teléfono celular sin autorización judicial, los propios órganos estatales incurrirían en un delito, como, por ejemplo, el de violación de secretos más arriba analizado, con la gravedad institucional que esto conlleva. Vale recordar que el Estado en modo alguno puede probar la comisión de un delito cometiendo otros, ya que de hacerlo, sus agentes se acabarían transformando en delincuentes. El principio de superioridad ética del Estado de Derecho indica que no corresponde convertir a la Administración de Justicia en beneficiaria de un hecho ilícito **(55)**.

Como acertadamente se ha dicho, "la Corte debería enfrentarse resueltamente contra la doctrina de que el fin justifica los medios y que el gobierno puede cometer crímenes para asegurar la condena del individuo" **(56)**.

Sin embargo, la única excepción que, a nuestro juicio, posibilitaría valorar en una decisión judicial un elemento probatorio colectado en violación a las garantías del imputado es cuando aquél lo favorezca, ello, con absoluta independencia de la eventual responsabilidad penal o administrativa que deba recaer sobre el funcionario infractor **(57)**.

Por otra parte, entendemos que, sin la intervención previa de un juez, el justiciable también podrá válidamente negarse a exhibirles a las fuerzas de seguridad o al órgano encargado de la persecución penal los contenidos del aparato que lo comprometen, toda vez que ello equivale tanto como a obligarlo a aportar pruebas en su contra, con serio perjuicio para la garantía que lo protege contra la autoincriminación forzosa.

La consecuencia procesal que acarrea cualquier declaración de nulidad, tanto en la Justicia de la Nación como en la Ciudad de Buenos Aires, concuerda con la extensión que emana de la teoría del fruto del árbol venenoso, ampliamente receptada por nuestra Corte Suprema.

Es por ello que si de la revisión ilegal o arbitraria de los contenidos de un teléfono móvil se obtuvieran fotografías, mensajes de textos, *e-mails* y/o grabaciones de voz que incriminen a la persona sindicada como autora de un delito, no sólo esos elementos de prueba serán inadmisibles para fundar una sentencia de condena, sino además todos los restantes a los que las fuerzas de seguridad hubiesen llegado como derivación directa de ellos, ya que éstos también se encontrarían contaminados por la misma ilegalidad inicial (cfr. arts. 172, CPPN y 75, CPPCABA) **(58)**.

En suma, creemos haber demostrado suficientemente a lo largo de este breve ensayo que los datos almacenados en los nuevos "*smartphones*" se encuentran amparados por las garantías constitucionales que protegen a los papeles privados y el derecho a la intimidad. En consecuencia, cualquier revisión que de ellos se pretenda hacer sólo podrá efectuarse por los medios y bajo las formas que los Códigos Procesales establecen, ya que de adverso, la prueba obtenida de ninguna manera podrá ser valorada en perjuicio del imputado a la hora de fundar una decisión judicial.

De todos modos, debemos reconocer que la regulación que actualmente rige la materia resulta harto insuficiente. De allí la importancia de que, a fin de superar las lagunas normativas ya reseñadas, la jurisprudencia de nuestros tribunales marque un rumbo que sea respetuoso de la naturaleza restrictiva de esta clase de injerencias, así como de los principios de subsidiariedad, mínima intervención y proporcionalidad exigibles en el marco de un modelo de Estado que, decididamente, considera razonable preservar el interés de los ciudadanos en mantener bajo reserva la información almacenada en sus aparatos inteligentes de telefonía celular.

(54) La Corte norteamericana en el caso "Silverthorne Lumber Co. v. United States" (1920) instauró la famosa teoría del fruto del árbol venenoso, por la cual la prueba ilegal obtenida contamina de ilicitud cualquier otra prueba derivada de ella. Esta teoría tuvo como fin principal proteger la intimidad, la dignidad y la libertad de los imputados, y evitar que el Estado se beneficiara de actos ilegales que él mismo cometiera, esto es, que no se aprovechase de lo que él mismo prohibía.

(55) Sobre esta cuestión, nuestra Corte en dos casos muy conocidos –"Montenegro" y "Fiorentino"– ha dicho: "...otorgar valor al resultado de un delito y apoyar sobre él una sentencia judicial, no sólo es contradictorio con el reproche formulado, sino que compromete la buena administración de justicia al pretender constituirla en beneficiaria del hecho ilícito (...)". Éstos son dos de los casos más emblemáticos en donde la Corte se expidió sobre la exclusión de los medios de pruebas obtenidos ilegalmente.

(56) Garibaldi, Gustavo, "Las modernas tecnologías de control y de investigación del delito", Ed. Ad-Hoc, Buenos Aires, 2010, p. 480.

(57) En efecto, como acertadamente sostiene el profesor Maier "...sólo basta la decisión favorable, pues ninguna garantía opera en perjuicio del propio portador" (cfr. "Derecho Procesal Penal", "I. Fundamentos", 2ª ed., 3ª reimpresión, Ed. del Puerto, Buenos Aires, 2004, p. 667.

(58) Para un minucioso análisis de algunas de estas cuestiones consúltese Carbone, Carlos A. "Requisitos constitucionales de las intervenciones telefónicas. Correspondencia telefónica, informática y audiovisual intervenida judicialmente en el proceso penal", Ed. Rubinzal-Culzoni, Buenos Aires, 2008.