

A actualización da LECrim ás necesidades da sociedade da información, erros e acertos

Ofelia Tejerina Rodríguez. Avogada da *Asociación de Internautas*.

O pasado 13 de Marzo o Consello de Ministros aprobou o Proxecto de Lei Orgánica de modificación da Lei de Axuízamento Criminal (LECrim no seu acrónimo en español) para o afortalamiento das garantías procesuais e as medidas de investigación tecnolóxicas, coa intención de adaptar as previsións normativas vixentes ás necesidades actuais da Sociedade da Información, algo que os internautas viñamos reclamando desde hai moito tempo.

Segundo a Exposición de Motivos, na parte da reforma que se está a acometer como Lei Orgánica incídese directamente nos artigos 18 e 24 da Constitución Española. Do primeiro dise que veñen desenvolver certos aspectos derivados do concepto de privacidade e do segundo, o que afecta directamente á súa garantía procesual, a tutela xudicial efectiva. Trátase en todo caso de medidas que desenvolven dereitos fundamentais, ou máis ben a súa restrición.

Tentaremos explicar os puntos que consideramos máis relevantes nesta materia, sen entrarmos tanto na forma (trasposición de determinadas Directivas Europeas) como no fondo. Concretamente analizamos as condicións que deberán darse: I.- para realizar escoitas autorizadas entre avogado e detido (arts. 520 e 118 LECrim); II.- a interceptación legal de todo tipo de comunicacións e o tratamento dos datos persoais dos afectados (art. 579 LECrim); III.- para o rexistro remoto de equipos informáticos (art. 588 LECrim); e finalmente, IV.- o papel do axente encuberto na persecución de determinadas modalidades delituosas (art. 282 LECrim).

I.- Escoitas entre avogado e detido (dereito de defensa)

Segundo sinala a Directiva 2013/48/UE do Parlamento Europeo e do Consello de 22 de outubro de 2013, os sospeitosos ou acusados teñen dereito a se reuniren en privado co seu Letrado e os Estados Membros teñen a obrigaón de respectaren a confidencialidade das súas comunicacións, excepto cando existir unha necesidade urxente de evitar graves consecuencias adversas para a vida, a liberdade ou a integridade

física dunha persoa; ou unha necesidade urxente dunha actuación inmediata das autoridades de instrución para evitar comprometer de modo grave o proceso penal. (estas excepcións amparan poder realizar interrogatorios mesmo sen presenza Letrada). Establécese que só baixo esas circunstancias e mediante autorización xudicial se pode prescindir desta confidencialidade, e tendo sempre en conta criterios de proporcionalidade, limitándose ao estritamente necesario e polo tempo preciso. A orde non poderá basearse exclusivamente no tipo ou a gravidade da presunta infracción, nin poderán ser menoscabadas as garantías xerais dun xuízo xusto. Esta restrición, tamén a recolle o Tratado da Unión Europea para supostos de Seguridade Nacional.

Baseándose nesa Directiva, a reforma española vén engadir á norma procesual que poida ser restrinxida a confidencialidade entre avogado e detido cando se constatar a existencia de indicios obxectivos da participación do avogado no feito delituoso investigado ou da súa implicación xunto co investigado ou procesado na comisión doutra infracción penal, porque se entende que unha actividade delituosa do Letrado non pode reputarse asistencia lexítima aos sospeitosos ou acusados.

O Tribunal de Xustiza das Comunidades Europeas na Sentenza (Gran Sala) de 14 de setembro de 2010 xa sinalou que a confidencialidade das comunicacións entre os avogados e os seus clientes debería ser obxecto de protección a nivel comunitario, con todo esa Directiva de 2013 permíteo en Europa e agora copiámolo aquí, talvez nun intento de precisarmos o que fixo o Xuíz Garzón na investigación do caso Gürtel, aínda que naquel caso concreto suponse que non foron encontrados indicios obxectivos suficientes de os Letrados teren aproveitado o exercicio da defensa para cometeren novos delitos.

Moitas foron as voces en contra de restrinxir así o dereito de defensa xa que, por lóxica pura, se o Letrado en cuestión está sob sospeita nunca deberían deixalo asistir a un detido, porque para comezar debe tratarse dun avogado independente. Por outra banda, se non existe unha relación de confianza entre cliente e Letrado, entre o sistema e os dereitos fundamentais dun Estado de Dereito, entón non existe garantía constitucional algunha nesta parte do proceso.

O Consello Xeral do Poder Xudicial (CXPX) no seu Relatorio de data 12 de Xaneiro de 2015, expresamente entende que esta garantía de confidencialidade debe ser aplicada tamén ás dilixencias policiais, e debe recollese así na norma.

II - A interceptación das comunicacións

A reforma procesual que se expón para o art. 579 esfórzase por precisar as circunstancias en que o dereito fundamental ao segredo das comunicacións (art. 18.3 CE) pode ser restrinxido. Segundo a Exposición de Motivos da proposta, trátase de acoutar o seu ámbito material de aplicación, regúlanse os prazos máximos de duración e as excepcións á necesidade de autorización xudicial de acordo cunha consolidada doutrina xurisprudencial.

Como é sabido, desde o ano 2005 a *Asociación de Internautas* estivo solicitando ao Goberno, ao Parlamento e ao Tribunal Supremo que precisasen este tipo de cuestións, polo avance das tecnoloxías na Sociedade da Información. Con todo, toda proposta de mellora foi ignorada até a data.

Basta deitar unha ollada aos aspectos desta materia que se foron denunciando e aos fundamentos legais, doutriniais e xurisprudenciais que se alegaban para impedir a entrada en vigor dunha regulación que considerábase do todo inconstitucional, e polos en relación con estas novas propostas de reforma, para ver que efectivamente non eran peticións arbitrarias, senón que eran do todo razoabeis e necesarias (<http://www.internautas.org/html/4895.html>). Mais tiveron que pasar 10 anos para o lexislador se dar conta da torpeza con viñera sendo regulada e interpretada esta materia, e para pór maos á obra comezando por precisar as restricións ao dereito fundamental ao segredo das comunicacións, á intimidade ou a protección de datos, tamén no que afecta á Sociedade da Información, mediante unha Lei Orgánica.

Ademais, coa reforma procesual parece que POR FIN se entende que a figura do xuíz debe estar presente desde o principio, desde a primeira actuación en materia de interceptación das comunicacións.

O CXPX así o viu, e así o recolle no seu Relatorio sobre a reforma ao destacar por exemplo que é necesaria a autorización xudicial para a cesión dos datos electrónicos conservados polos prestadores de servizos ou persoas que faciliten a comunicación (artigo 588 bis p), que viña imposta polo artigo 1.1 da Lei 25/2007, de 18 de outubro, de conservación de datos, e recoñecida por un Acordo do Pleno non xurisdiccional da Sala Segunda do Tribunal Supremo de 23 de febreiro de 2010. E aplaude que agora veña a establecer debidamente nunha Lei Orgánica, e coas precisións que era necesario recoller, pois contribúe a realizar o principio constitucional de seguridade xurídica (artigo 9.3 CE) e con iso a calidade e excelencia da lei no que implique intervención sobre os dereitos fundamentais, tal e como é concibida pola xurisprudencia do TEDH.

O CXPX menciona neste punto que moi recentemente, a Sala Segunda do Tribunal Supremo (TS), na súa sentenza 850/2014, de 26 de novembro, puxo de manifesto a ausencia de regulación legal expresa da intervención das comunicacións telemáticas, e da necesidade de colmatar esa lacuna coa máxima urxencia, dada a relevancia dos dereitos fundamentais e intereses xerais en conflito. Di que a doutrina xurisprudencial –segundo precisa a referida sentenza- realizou un considerábel esforzo para emendar este déficit (...).

E isto é moi curioso, porque tanto o referido acordo do Pleno do TS non xurisdicional, como esta última Sentenza, son posteriores á Sentenza do propio Tribunal Supremo de data 5 de Febreiro de 2008 (Sentenza: http://www.internautas.org/archivos/pdf/sts_interceptacion_comunicacione_s.pdf), unha resolución que foi resultado da impugnación da norma coa que veu a desenvolver esta materia na altura (<http://www.internautas.org/pagweb/15.html>) e que estivo vixente até agora.

A *Asociación de Internautas* denunciou en 2005 esas mesmas carencias normativas e a necesidade dunha regulación expresa, precisa, e constitucionalmente amparada nunha lei orgánica. Con todo, o TS considerou que todo fora lexitimamente resolvido coa aprobación da Lei 25/2007 de conservación de datos relativos ás comunicacións electrónicas e ás redes públicas de comunicacións, que sinala que o tratamento dos metadatos asociados a un usuario requiría autorización xudicial previa.

Especial mención mérecenos precisamente agora o exposto no Voto Particular do Maxistrado Óscar Gómez Gómez, a cuxa lectura nos remitimos para que se dean conta de como estaba o patio nestas cuestións hai 7 anos, e que, a pesar das explicacións lóxicas e xurídicas que xa se imploraban sobre a necesidade de que esta materia fose precisada nunha lei orgánica, ou que non podía desxudicializarse a medida de interceptación nin sequera a respecto dos datos de tráfico, nada se fixo, tampouco xurisprudencialmente.

Sobre estes datos de tráfico asociados, o lexislador POR FIN parece comprender que, en cumprimento dos principios de excepcionalidade, especialidade, idoneidade, necesidade e proporcionalidade na medida, que non son unha cuestión fútil, imponse a esixencia de autorización xudicial para a súa cesión aos axentes facultados, sinalándose expresamente que a súa incorporación ao proceso só será autorizada cando se tratar da investigación dun delito que, por razóns vinculadas ao principio de proporcionalidade, for dos que xustifican o sacrificio da inviolabilidade das comunicacións. Aínda que se regula separadamente o suposto da cesión de datos desvinculados dos procesos de comunicación concernentes á

titularidade ou identificación dun dispositivo electrónico, aos que poderá acceder o Ministerio Fiscal ou a Policía Xudicial no exercicio das súas funcións sen necesidade de autorización xudicial. Este concepto de datos desvinculados non está claro, e podería contradicir mesmo outras previsións da norma.

O CXPX pon de relevo que nos casos en que for precisa a colaboración das operadoras, para a cesión dos datos de identificación e localización do equipo e os datos de identificación persoal do usuario a partir dunha dirección IP á que a Policía Xudicial puider ter acceso nun rastrexo policial do espazo público, esta orde de colaboración debe provir do Xuíz. Entende que para a identificación do titular dun IP é precisa a orde xudicial, e que o mesmo debería esixirse para a identificación após unha actividade de monitorización, rastrexo ou captación do IMSI ou do IMEI.

Pola súa banda, o Consello de Estado tamén se pronunciou e considera no seu Relatorio de 9 de Marzo de 2015 que o IP, o IMSI ou o IMEI son datos persoais (a respecto das posibilidades de inxerencia ilícita na intimidade do usuario se este non é identificado sob mandato xudicial). Di literalmente que a cesión de tales datos polas operadoras para identificación do usuario require autorización xudicial, aínda que sorprende cando di que a reforma peca dun excesivo garantismo, pois hai casos en que a identificación pode ser necesaria de forma previa, para poder pedir a orde xudicial de interceptación. Aquí preguntámonos se non se pode pedir a identificación e a interceptación das comunicacións que se corresponden cun número concreto na mesma solicitude policial que xorde desa investigación penal. Salvo que se pretenda ir adiantando traballo ao xuíz, non se comprende esta afirmación.

Outras cuestións que se vén ordenar con esta reforma son os límites temporais destas medidas, eses tres meses que en principio poden ser prolongados até un máximo de dous anos, se subsistiren as causas que motivan a medida. Dise na Exposición de Motivos que o lexislador quere evitar que se prolonguen de forma innecesaria a interferencia dos poderes públicos na privacidade dos cidadáns afectados pola medida, e por iso di tamén que non é tolerábel a petición sistemática das medidas de inxerencia. Mais o CXPX critica ese prazo máximo de dous anos, en consideración á necesidade de preservar o principio de especialidade e evitar intervencións prospectivas, e tamén, por coherencia cos límites que inclúe a propia reforma á duración da fase de instrución, o que sen dúbida compartimos.

A respecto da autenticidade e integridade dos soportes postos a disposición do xuíz, a reforma impón a utilización dun sistema de carimbado ou sinatura electrónica que garanta a información transferida desde o sistema central. E prevé tamén un precepto destinado a fixar os termos do borrado e

eliminación das gravacións orixinais, unha vez se puxer termo ao procedemento. Preténdese con iso evitar toda difusión dun material que, polo seu propio contido, podería danar de forma irreparábel a intimidade do afectado.

En xeral a reforma positiviza a idea de que sexa un xuíz quen ordene este tipo de medidas, sempre ponderando a gravidade do feito obxecto de investigación, precisando o ámbito obxectivo e subxectivo da medida, e mesmo os requisitos que deben ser observados na solicitude policial de intervención.

O CXPX, após un repaso á xurisprudencia recaída na delimitación dos conceptos intimidade, segredo das comunicacións e protección de datos, en relación coa interceptación das comunicacións, lembra que esta medida fica reservada aos delitos de maior gravidade e cunha finalidade exclusivamente probatoria (sempre que non existir unha posibilidade menos gravosa) da existencia do delito e das persoas responsabeis do mesmos, sen que sexan lícitas as medidas de investigación acordadas con carácter prospectivo, por sospeitas ou conxecturas, nin para tratar de descubrir de maneira xeral e indiscriminada actos delituosos. E lembra que debe ser adoptada no seo dun proceso de investigación penal e mediante resolución xudicial suficientemente motivada, o que advirte tamén o Consello de Estado no mesmo sentido, aínda que di que non lle parece lícito que os orzamentos delituosos para poder adoptar medidas de investigación que son todas invasivas nos dereitos fundamentais do art. 18 da CE, sexan tan diferentes. Por exemplo, que para a apertura de correspondencia postal se esixa que haxa indicios de obter por este medio o descubrimento dalgún feito ou circunstancia relevante para o caso, mentres para a interceptación das comunicacións debe estarse perante a comisión (ou sospeita) de delitos castigados con penas de mínimo tres anos de prisión, delitos de terrorismo, ou de delincuencia de bandas organizadas. Defende este organismo unha cláusula máis xeneralista e menos casuística, mais non se pode comprender esta petición por motivos de seguridade xurídica. Aínda que se trate de medidas que afectan dereitos fundamentais recollidos no mesmo precepto constitucional, non pode deducirse por iso que deban ter o mesmo tratamento procesual nin as mesmas cautelas, pois nada ten que ver a entrada nun domicilio concreto, coa apertura da correspondencia postal, nin cun tratamento de datos persoais ou unha interceptación de comunicacións electrónicas, por canto se intervén en lugares ou en condutas, cos límites temporais, espaciais e subxectivos (persoas que poden resultar afectadas coa medida) que iso require.

O CXPX sobre este aspecto aconsella plasmar positivamente o principio de proporcionalidade e establecer con precisión os delitos que poden xustificar a inxerencia, especialmente nos supostos en que non for preceptiva a

autorización xudicial, é dicir, casos de urxencia, cando as investigacións se realizaren para a investigación de delitos cometidos no seo de organizacións criminais, delitos de terrorismo, delitos contra menores ou persoas con capacidade modificada xudicialmente ou outros delitos que, en virtude das circunstancias do caso, poideren ser considerados de especial gravidade e existiren razóns fundadas que fixeren imprescindíbel a intervención das comunicacións. Nestes casos, a norma autoriza o Ministro do Interior, e na súa falta o Secretario de Estado de Seguridade, a acordar a medida de investigación pertinente, que será comunicada inmediatamente ao Xuíz e, en todo caso, dentro do prazo máximo de 24 horas, facendo constar as razóns que xustificaron a adopción da medida. Entende que esta previsión expón serias dúbidas de encaixe constitucional porque o artigo 55.2 CE só se refire á suspensión do dereito ao segredo das comunicacións nos casos de bandas armadas ou terrorismo, o que resulta do todo razoábel advertir pois os límites e garantías constitucionais sobre os supostos en que cabe a suspensión de cada tipo de dereito fundamental son diferentes.

O CXPX critica por isto que se amplíe o elenco dos delitos respecto dos que se permite a inxerencia a aqueles cometidos contra menores ou persoas con capacidade modificada xudicialmente ou outros delitos que, en virtude das circunstancias do caso puideren ser considerados de especial gravidade, sen fixar sequer os elementos obxectivos conforme aos cales pode e debe facerse esa cualificación, que fica en mans da discrecionalidade das autoridades gubernativas.

Outro apartado co que se mostra moi crítico este organismo, é o que prevé as intervencións de comunicacións que se practicarán en segredo, sen necesidade de se acordar expresamente o segredo da causa, pois considera que o precepto non permite descubrir que é o pretendido polo prelexislador, e como cabe articular tal previsión, polo que é necesario que se estableza con claridade o sentido da norma e a forma de levar a efecto a disposición que contén, o que se comparte plenamente.

Advirte tamén do risco que representa para o contido constitucional do dereito á intimidade persoal e ao segredo das comunicacións, a posibilidade de solicitar a información que conste nos arquivos automatizados dos prestadores de servizos, incluída a procura entrecruzada ou intelixente de datos, sempre que se precisar a natureza dos datos que houberen ser coñecidos e as razóns que justificaren a cesión. Di que será a práctica a que poña de manifesto a dificultade de cumprir os supostos que habilitan a cesión dos datos obtidos a través de ligazóns ou “links”, así como a eventual transgresión dos principios que informan a regulación da interceptación das comunicacións, polo que agora só cabe advertir do risco detectado nun plano meramente teórico.

Medo danos a práctica, cando ademais o propio CXPX di que resulta pouco explicábel incluír uns apartados cun elevado risco de conflito constitucional cando existe un sistema xudicial organizado para dar resposta inmediata a este tipo de solicitudes de intervención. E critica tamén que se utilicen termos tan pouco precisos como transcendencia social e caso de urxencia, para afastar o xuíz da decisión de utilizar estas medidas.

A conclusión, como sinala o CXPX, é que coa reforma (POR FIN) colmátase a esixencia da necesaria cobertura legal das medidas de intervención, e sométese en todo caso, e con carácter xeral, a licitude da intervención á concorrencia dos principios de especialidade, excepcionalidade, idoneidade, necesidade e proporcionalidade da medida, xunto cos que, ao longo do desenvolvemento do articulado, o texto plasma tamén de forma positiva, como o que impón o deber de motivación da resolución que acorde a intervención e a súa prórroga, a súa limitación temporal e o control xudicial da súa execución.

O CXPX con todo, resta importancia as escoitas realizadas co sistema SITEL, e di que fican á marxe desta norma. Non se comprende moi ben en que se basea, ou a que aspectos se refire, xa que parece basearse simplemente no respaldo xurisprudencial ao feito de a tecnoloxía de SITEL ser legal (plenas garantías que ofrece o Sistema Integrado de Interceptación de Telecomunicacións (SITEL), di), desvinculándoa do uso ou mal uso que se fai coa información captada, mesmo coa anuencia da deficiente lexislación actual, que, por outra banda, si é recoñecida como deficiente por todos os axentes que a analizaron para a súa reforma.

Outra cuestión á que resta importancia son os límites temporais da xeovixilancia, ou que se limitase só a delitos graves, porque di que é de pouca relevancia a afectación do dereito á intimidade con esta medida (só se vé afectado o dereito á intimidade e en escaso grao), e que para iso xa están os principios de proporcionalidade e a intervención xudicial. Ningún destes argumentos pode ser compartido se temos en conta o alcance deses sistemas de xeolocalización, e a cantidade de aspectos da vida privada dunha persoa (e terceiros próximos) que pode revelar, e é que, como di o Consello de Estado, dependendo do ben en que for instalado o sistema de seguimento (*excepcionándose os supostos de acreditada e urxente necesidade relacionados coa investigación penal), verase afectada a intimidade e vida privada do suxeito en maior ou menor medida e isto non pode afastarse das garantías da CE.

III - O rexistro remoto de equipos informáticos

A reforma da LECrim. recolle a opción de as autoridades policiais poderen proceder ao rexistro de dispositivos informáticos de almacenamento masivo e ao rexistro remoto de equipos informáticos. Sob mandato xudicial as autoridades policiais poderán “instalar software que permita de forma remota e telemática, o exame a distancia e sen consentimento do seu titular ou usuario do contido dun computador, dispositivo electrónico, sistema informático, instrumento de almacenamento masivo de datos informáticos ou bases de datos.”

O rexistro remoto de computadores faríase co que se nos quere vender como “troyanos bos”, e dise que serán utilizados en supostos de:

- a) Delitos cometidos no seo de organizacións criminais.
- b) Delitos de terrorismo.
- c) Delitos cometidos contra menores ou persoas con capacidade modificada xudicialmente.
- d) Delitos contra a Constitución, de traizón e relativos á defensa nacional.
- e) Delitos cometidos a través de instrumentos informáticos ou de calquera outra tecnoloxía da información ou a telecomunicación ou servizo de comunicación.

Independentemente de que ese último apartado nos pareza unha idea terrorífica para calquera Estado de Dereito, é incríbel que ademais se estableza dunha maneira tan vaga, sen precisións de ningún tipo, e creando unha inseguridade xurídica absoluta sobre os supostos de feito en que se poderán utilizar. Entendemos que é de maneira evidente inconstitucional, porque non contén xustificación de proporcionalidade nin concreción algunha da súa finalidade (só di descubrir delitos en Internet) a respecto dos dereitos fundamentais que así quedarán conculcados. Calquera proba así obtida, sexa ordenada ou non por un xuíz, non pode ter cabida nun proceso penal xusto que queira respectar as garantías da debida tutela xudicial efectiva.

Segundo o CXPX, o lexislador ten unha maior liberdade de configuración sobre o dereito á intimidade, e por iso, non se coloca dúbidas de constitucionalidade a ese respecto “nos casos de emerxencia ou risco de catástrofe ou cando a medida teña por obxecto a localización de persoas en situación de urxencia vital”. Con todo, noutro tipo de casos, di que hai que ter en conta que esta medida “afecta non só datos concretos concernentes ao sospeitoso, senón en xeral o exame a distancia e sen coñecemento do seu titular ou usuario da totalidade do contido dun computador, dispositivo electrónico, sistema informático, instrumento de almacenamento masivo de

datos ou base de datos, explica, por unha banda, a expresa submisión da medida aos principios xerais que inspiran a regulación das medidas de inxerencia nos dereitos consagrados no artigo 18 CE –particularmente aos principios de idoneidade, necesidade e proporcionalidade–, e por outra, que sexa reservada a delitos de especial gravidade”.

Este organismo pide no seu Relatorio sobre a modificación “que se defina con maior precisión o que debe entenderse por delitos de especial gravidade a estes efectos, establecendo sequera aqueles elementos de carácter obxectivo que sirvan de pauta interpretativa para colmatar o concepto insuficientemente determinado”, mais o certo é que primeiro habería que limitar expresa e literalmente a medida a delitos informáticos de especial gravidade, e xa despois definir isto, porque no último rascuño coñecido, de data 13 de Marzo de 2015, a proposta de artigo 588 septies a., non recolle ese concepto de especial gravidade, permitíndose sen máis os rexistros remotos para todo tipo de delitos cometidos a través de instrumentos informáticos. Entre outras cuestións, tampouco recolle expresamente límites xeográficos.

Sobre esta proposta de rexistro en liña de computadores, en xeral, é preciso lembrar que o Tribunal Constitucional de Alemaña, anulou no ano 2008 a reforma da Lei dos Servizos de Intelixencia do Estado Federal de Renania no Norte Westfalia, que pretendía facer practicamente o mesmo que aquí. Consideraba a idea inconstitucional, aínda limitándose a sospeitosos de terrorismo, e fixébase por primeira vez o dereito ao respecto e a integridade de sistemas informáticos.

Segundo o Tribunal alemán aquela norma non cumpría “nin a regulación do limiar de lesión, nin os requisitos procesuais dos elementos da devandita lesión”, o que acontecía tamén na reforma da norma española, a respecto da nosa propia CE. Non se cumprían os requisitos constitucionalmente exixíbeis de respecto aos dereitos fundamentais que poderían verse lesionados cunha medida deste tipo, e sinalaba que “as medidas de vixilancia secretas realizadas por organismos estatais deben respectar unha área central inviolábel da vida privada”, porque “o desenvolvemento da personalidade na área central da vida privada inclúe a posibilidade de expresar acontecementos internos como percepcións e sentimentos, así como consideracións, opinións e experiencias dunha natureza altamente persoal, sen temer que organismos estatais poidan ter acceso a eles”. Recoñeceu este Tribunal que “no caso de acceso secreto ao sistema de tecnoloxías da información do interesado, existe unha necesidade de precaucións especiais establecidas pola lei que protexen a área central da vida privada”, e anulaba as disposicións impugnadas por ficar sobradamente acreditada unha “lesión do dereito xeral á personalidade na

súa manifestación da protección da confidencialidade e da integridade de tecnoloxías da información”.

Pero en España, como é habitual, imos por libre.

IV - O axente encuberto

O axente encuberto é unha figura que aparece coa modificación da LECrim en 1999, delimitada para investigación e persecución da delincuencia organizada. Coa nova reforma quérese introducir novos supostos de feito lexitimadores da súa intervención, concretamente interéranos o que se refire a feitos que se produzan en canles pechados de comunicación telemática.

A proposta establece a posibilidade de “o axente encuberto electrónico poder intercambiar ou enviar por si mesmo arquivos ilícitos, sendo posíbel en tal caso a análise dos algoritmos asociados aos devanditos arquivos”. E na Exposición de Motivos explícase que “a necesidade de autorización xudicial garante o pleno respecto do dereito á intimidade e ao segredo das comunicacións das persoas afectadas”.

Na análise da cuestión o Consello de Estado, coincidindo co CXPX e co Consello Fiscal, entende que é necesario contar con autorización xudicial previa para este tipo de intervencións en supostos de troca de arquivos ilícitos, precisamente polo concepto de ilícito. É máis, o Consello Fiscal cre inconstitucional a posibilidade de o Ministerio do Interior decidir a intervención das comunicacións para investigar delitos de especial gravidade sen autorización xudicial previa. Aínda que agora pode tomar estas decisións “mediante resolución fundada e tendo en conta a súa necesidade aos fins da investigación”, e en todo caso, dando conta inmediata ao Xuíz.

A actual regulación da LECrim di que o axente encuberto non pode provocar ou inducir a cometer unha conduta puníbel, que non pode vulnerar bens xurídicos superiores aos da conduta delituosa obxecto da investigación nin atentar contra a vida e a integridade das persoas. E di que “estará exento de responsabilidade penal naquelas actuacións que foren consecuencia necesaria do desenvolvemento dunha orde lexítima, sempre que esta actuación garde a proporcionalidade”.

É dicir, até agora suponse que o papel do axente encuberto limitábase a obter probas para a condena dos delitos investigados, mais o que se introduce agora é máis ben outra figura, a que é coñecida pola xurisprudencia como o “axente provocador”.

Segundo a STS 53/97, de 21 de xaneiro, estes axentes provocadores realizan condutas que “sen conculcaren legalidade algunha, encamiñanse ao descubrimento de delitos xa cometidos, xeralmente de tracto sucesivo como adoitan ser os de tráfico de drogas, porque en tales casos os axentes non procuran a comisión do delito senón os medios, as formas ou canles polos que ese tráfico ilícito se desenvolve, é dicir, preténdese a obtención de probas en relación a unha actividade criminosa que xa se está producindo mais da que unicamente se abrigan sospeitas”.

Olo, esta figura é diferente da que intervéñen no “delito provocado”, polo momento en que o investigado toma a decisión de delinquir. Se o investigado xa tiña a decisión de cometer un ilícito, entón (segundo a xurisprudencia) o axente non provoca, non engana, nin manipula a súa vontade, o que fará é tomar medidas para descubrir o delito, e no caso do que agora falamos, para descubrir as canles polas que veñen intercambiando os arquivos ilícitos con anterioridade.

Nos supostos de tráfico de drogas, expónse o feito de que un axente venda sustancias ilícitas e cobre por iso, e dise que isto é diferente a que simplemente as ofrezca, sen chegar a producirse a venda. E se o axente se presentar como suposto comprador, sen chegar a terminar a operación, caberían aínda menos dúbidas sobre a súa lexitimidade.

Estas son as explicacións xurisprudenciais á nova figura á que nos enfrontamos, con todo, na formulación da reforma, o difícil será que o órgano xurisdiccional determine cando se produciu a actuación espontánea e de modo natural dos delincuentes, ou se o axente se valeu de manobras capciosas ou enganos polo mero feito de cargar contidos ilícitos na rede, e iso, polo funcionamento propio das redes de troca de arquivos. Se os axentes poñen arquivos ilícitos a disposición de terceiros, o seguinte que cabe esperar é a súa descarga (digamos a adquisición da droga, se falásemos de delitos contra a saúde pública), por tanto, poderíase falar de “provocación” no seu sentido estrito e ilícito. Aínda que sempre poden dicir que os axentes subiron os arquivos só para se poren en contacto con sospeitosos de distribución dos mesmos, mais ten complicado encaixe.

Esta nova figura talvez podería salvarse nos supostos de troca de arquivos de pornografía infantil mais, por exemplo, respecto de ilícitos contra a propiedade intelectual, parece imposible e absurda pois a descarga de arquivos protexidos por dereitos de autor en redes P2P para uso doméstico, non é ilícito (e menos delito), de maneira que nunca estaría xustificada esta intervención.

A infiltración dun axente, cando se restrinxen dereitos fundamentais, como os dereitos á intimidade ou ao segredo das comunicacións que amparan a

troca de arquivos en liña, debe en todo caso ser autorizada polo Xuíz de Instrución competente, sob os seguintes criterios:

- a. Existencia de indicios suficientes
- b. Idoneidade da medida
- c. Necesidade ou subsidiariedade da medida
- d. Gravidade da conduta investigada
- e. Motivación

Como se dixo, no caso da propiedade intelectual deberán xustificarse indicios suficientes de que unha banda organizada descarrega arquivos protexidos por dereitos de autor para despois lucrar con iso, xa que doutra maneira non tería xustificación constitucional algunha a adopción desta medida.

Á hora de legislar condutas propias de Internet, deben terse en conta como funciona, neste caso, como funcionan as redes P2P, en relación coa xurisprudencia interpretativa dos conceptos que se lle queira aplicar, para asegurarse ben de que existen garantías constitucionais na súa regulación. Neste caso concreto:

“que o engodo posto en xogo polos investigadores vaia dirixido non á promoción do suposto delito, índice e contraste da tenibilidade dos destinatarios da incitación, senón a patentizar e descubrir situacións ou actividades criminais até esa altura ocultas, mais xa existentes e, en consecuencia, puníbeis, sen que a nota positiva ou negativa, de espontaneidade a respecto do acto último, meramente revelador do delito, afecte á realidade certa do mesmo” (Sentenza TS, de 18 de Abril de 1972).

Por último, sinalar que o CXPX entende no seu Relatorio sobre a reforma que “resulta aconsellábel someter tamén de forma expresa a intervención do axente encuberto informático á autorización xudicial para a análise dos algoritmos asociados aos arquivos ilícitos que envíe ou troque o axente encuberto”.