ACÓRDÃOS DO TC N.os 213/2008 E 486/2009: A PROVA NUMA SOCIEDADE TRANSPARENTE [1]

LUÍSA NETO [*]

I. UM NOVO DIREITO OU UM NOVO OBJECTO PARA O DIREITO?

1. A zona de afectação radical dos indivíduos está na *terra incognita* da experiência subjectiva. Ora, já em 1998, se lia num artigo do semanário Expresso: "[N]um mundo urbano esquadrinhado por milhares de

---

[1] As questões suscitadas por estes Acórdãos não se apartam daqueloutras tratadas por Maria Fernanda Palma, *Tutela da vida privada e processo penal*, Jurisprudência Constitucional, n.º 10 — Abril — Junho 2006, e Paulo Mota Pinto, *A protecção da vida privada no Tribunal Constitucional*, Jurisprudência Constitucional, n.º 10 — Abril — Junho 2006. Ainda na mesma esfera de preocupações, lembre-se Manuel da Costa Andrade, *Domicílio, intimidade privada e constituição,* Revista de Legislação e Jurisprudência, n.º 3953, Novembro/Dezembro de 2008. Se ora se faz alguma actualização para efeitos do que se pode denominar por telemetria, e ainda que nos guardemos de ser profetas, dir-se-á que não é difícil adivinhar que as próximas decisões do Tribunal Constitucional em temáticas circundantes estarão necessariamente relacionados com os métodos biométricos, que podem ser definidos como a medida e a análise de características da biologia humana. A força com que, nestes últimos anos, o assunto se desenvolveu fez nascer duas ilusões: a de que é muito recente e a de que apenas tem a ver com valores como os da liberdade, a privacidade e a segurança — nomeadamente resultante do denominado direito penal do inimigo surgido dos escombros do 11 de Setembro. O estado da arte da biométrica pode ser acompanhado em Ravi Das, *An introduction to biometrics*, Military Technology, 29 (2005), págs. 20-27; S. Garfinkel, *Database Nation,* Sebastopol, CA, O´Reilly, 2002; John Gibb, *Who's Watching You?*, London, Collins & Brown, 2005; David Lyon, *Surveillance after September 11,* Cambridge, Polity, 2003; e John D. Woodward, Jr., *Biometrics*, Santa Monica, CA, RAND, 2001.

[*] Prof. Associada da Faculdade de Direito da Universidade do Porto

câmaras de vídeo, onde o dinheiro digital e os cartões de crédito constituem um livro aberto sobre a intimidade de cada um, em que os "olhos"indiscretos dos satélites podem ler a matrícula de um carro e no qual os "media" apelam a um voyeurismo permanente, não admira que a privacidade seja, cada vez mais um conceito em vias de extinção."

Sendo a República Portuguesa um Estado de Direito baseado no respeito e na garantia de efectivação dos direitos e liberdades fundamentais dos cidadãos, impõe-se *hoc casu* uma delimitação do poder estadual de ingerência quer através da previsão de que a integridade moral das pessoas é inviolável, e de que a todos são reconhecidos os direitos à identidade pessoal e à reserva da intimidade da vida privada, quer determinando garantias efectivas contra a obtenção e utilização abusiva da informação relativa às pessoas e às famílias (artigos 25.º, n.º 1, e 26.º, n.os 1 e 2, e 34.º da CRP), ou dos dados considerados 'sensíveis' (artigo 35.º da CRP).

2. Mas no âmbito de uma sociedade transparente — expressão proposta por David Brin (*The Transparent Society,* Addison Wesley) em 1998 — qual é o conteúdo abrangido pela "vida privada" e que não resulta evidente, ao menos em termos definitivos, das previsões constitucionais referidas? Em 1890, o juiz norte-americano *Louis Brandeis* propunha — definindo-o como *the most valued by civilized men — the right to be let alone,* fazendo-o corresponder, essencialmente, ao direito que assistia a cada indivíduo, de ser deixado em paz. Entendia-se aqui pressuposta a necessidade da existência de um "espaço vital" onde cada um se pudesse sentir ao abrigo da indiscrição alheia, que nos remete para a *privacy* e ainda, garantisticamente, para a autodeterminação informacional e para a protecção de ingerência abusiva em formas hodiernas de comunicação.

Ora, numa sociedade de informação, não parece que possa aprioristicamente fazer-se uma enumeração completa e indiscutível do conteúdo da vida privada objecto de protecção, nem o legislador teve essa pretensão, utilizando uma cláusula geral e afastando qualquer susceptibilidade de taxatividade, como realçaram os Pareceres do Conselho Consultivo da Procuradoria Geral da República de 1980 e 1983.

Partindo de uma delimitação que separa o cidadão em si mesmo da sua vida em relação [(2)], um conhecido autor inclui no conteúdo do direito

---

[(2)] Veja-se, por todos, Luis Fariñas Matoni*, El derecho a la intimidad*, Editorial Trivium, Madrid, 1983.

à reserva, em primeiro lugar o que se refere ao cidadão em si mesmo, quer por referência ao passado — que pode ser evocado no presente, contra a vontade do próprio —, quer por referência ao presente, quer ainda por referência aos planos ou projectos de futuro. Esta noção integra o direito de se opor às ingerências de outrem — simultaneamente previsto como direito fundamental e como direito de personalidade —, mas não ficam por aqui as possibilidades de enriquecimento do conceito, a pressupor elaboração doutrinal e jurisprudencial permanentes, nomeadamente num tempo em que provavelmente o desenho de uma esfera autónoma de realização de cada cidadão resulta tão ou mais ameaçado em termos que decorrem da eficácia horizontal — da comunidade — do que as que tradicionalmente correspondiam às ameaças estaduais — eficácia vertical. (3)

No entanto, a evolução dos meios tecnológicos passíveis de colidir com a vontade de o indivíduo controlar a informação que sobre si existe na comunidade introduz problemas novos na configuração seja da *privacy*, seja da protecção de dados pessoais a que não bastam as referências difusas à intimidade e à protecção e reserva da vida privada.

Assim, mais de um século depois daqueloutra formulação adiantada por Brandeis na última década do Século XIX e quase meio século depois do desenvolvimento logrado também na Alemanha, mesmo se a formulação parece ainda exprimir uma evidente sensatez, é cada vez mais difícil de perceber como poderá ser assegurado na sua totalidade esse "direito a ser deixado sózinho".

Recorde-se que, ao proceder à distinção entre a reserva *lato sensu* e a *privacy,* o Tribunal Constitucional Alemão veio introduzir a ideia de autodeterminação, abrangendo o direito de fazer escolhas essenciais numa esfera de intimidade e segredo, na medida em que a divulgação intempestiva de factos próprios do sujeito possa ameaçar o exercício efectivo de outras liberdades. Neste sentido, é aí possível a distinção entre o conceito de intimidade — equivalendo ao segredo e factos ocultos — e o de privacidade — correspondendo aos conceitos de "riservatezza" italiana ou de "privacy" anglo-saxónica.

De facto, se em Itália distingue a doutrina entre esferas concêntricas de protecção que abrangem a intimidade (pessoal e familiar) e a vida privada, e que distinguem sucessivamente os conceitos de solidão — a

---

(3) Rita Amaral Cabral, *O direito à intimidade da vida privada*, in Estudos em memória do Prof. Paulo Cunha, Lisboa, 1988, págs. 373 a 406.

susceptibilidade de evitar contacto físico —, a intimidade — a susceptibilidade de reduzir contactos a grupos reduzidos —, o anonimato — do individuo que ainda que exposto a contactos mantém liberdade — e finalmente a reserva entendida em sentido próprio — enquanto possibilidade de banir intromissões não desejadas; nos EUA, o objecto de tutela desta liberdade centra-se essencialmente neste último vector de segurança frente a intromissões indevidas, visando essencialmente salvaguardar a garantia de respeito por opções pessoais, a liberdade de escolha sem interferências e a proibição de acesso a informação.

3. Se o objecto da privacidade é, certamente, polimorfo, o 'direito a ser deixado só' parece conferir à liberdade da vida privada o elemento de abstracção ou de indeterminação que caracteriza todas as outras liberdades públicas: a inserção da vida privada num círculo de relações humanas diversificadas transmuta a liberdade ética numa liberdade jurídica e instrumentalmente protegida.

É certo que, ao invés do que muitas vezes se entende agitar como bandeira, não obstante a sua aplicabilidade directa e a sua vinculação de entidades públicas e privadas, os direitos liberdades e garantias são passíveis de restrição, nos termos constitucionalmente adequados, quais sejam os de se visar a concordância prática para a resolução de uma colisão entre este direito e um bem jurídico da comunidade ou do Estado — *v. g.* para a realização da justiça, como ora nos interessa — ou de um conflito entre dois ou mais direitos fundamentais com distinta titularidade, e desde que se manifestem cumpridos os pressupostos da intervenção legislativa proporcional e não retroactiva, e que se não atinja o núcleo mínimo essencial da previsão jusconstitucional.

E recorde-se que há muito já se abandonou um critério hierárquico de solução de conflitos e colisões: o referido critério da concordância prática incide sobre o tipo e intensidade da lesão em causa, que pode muitas vezes ser mínima, ancorado fortemente no princípio da proporcionalidade nas suas três vertentes: necessidade, adequação e proibição do excesso.

Aliás, da mera sistematização constitucional se retira a possibilidade da consideração de limites imanentes, restrições implícitas, ou das chamadas teorias de *Tatbestand* alargado ou da conversão — todas estas expressões que de originalidade têm apenas a forma, porquanto sempre se referem à inevitabilidade de compatibilização hermenêutica interna do texto constitucional.

4. Como se disse, é por demais evidente que uma das matérias hoje mais sensíveis quanto à delimitação ordinária da protecção da vida privada se encontra no conceito de "intimidade informática" ou de "autodeterminação informacional" a que se refere o artigo 35.º da CRP [4], ganhando dimensão instrumental para o que ora nos interessa, na protecção do artigo 34.º [5] e do n.º 8 do artigo 32.º

A recolha de dados pessoais (não importando, *hoc casu*, o seu suporte) — e o seu tratamento automatizado quando referentes a "convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada" — encontra-se proibida em termos absolutos pela CRP e pela lei ordinária e, em termos relativos quando referentes à "origem étnica, condenações em processo criminal, suspeitas de actividades ilícitas, estado de saúde e situação patrimonial e financeira". Mas, esta última proibição é, em grande medida, desvirtuada pelas excepções que admite — reconhecidas desde a Convenção do Conselho da Europa para a Protecção dos Indivíduos face ao Tratamento Automático de Dados Pessoais (1981) e das Directrizes da OCDE sobre a Protecção da Vida Privada e os Fluxos Transfronteiras de Dados Pessoais (1981) quer ainda,

---

[4] O referido preceito consagra a protecção dos cidadãos perante o tratamento de dados pessoais informatizados, tendo vindo a ser objecto de profundas remodelações pelas sucessivas revisões do texto constitucional. Um dos fulcrais instrumentos jurídicos de garantia é a proibição contida no n.º 4 do artigo 35.º da CRP, que, como regra, veda o acesso aos dados pessoais de terceiros, de forma a impedir a sua devassa.

[5] Com efeito, nos termos prevenidos nos n.os 1 e 4 do artigo 34.º da CRP, o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis, sendo proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.

A proibição da ingerência abarca a liberdade de envio e de recepção de correspondência — *id est,* não apenas o conteúdo como o tráfego *a se* — e a proibição de retenção ou de apreensão, bem como de interferência, que se estende não apenas às entidades públicas mas também, e por maioria de razão, às entidades privadas.

As restrições estão assim autorizadas apenas em processo criminal e estão igualmente sob reserva de lei (artigo 18.º, n.os 2 e 3), só podendo ser decididas por um juiz (artigo 32.º, n.º 4).

Por força do estatuído no n.º 4 daquele artigo 34.º, o direito ao sigilo das telecomunicações envolve a proibição da devassa do seu conteúdo e a sua divulgação por quem a elas tenha acesso, designadamente os empregados dos serviços de telecomunicações, para quem decorre um dever de sigilo profissional, como garantia do direito ao sigilo das mesmas telecomunicações, que não poderá ser violado.

em definitivo, pelas sucessivas Directivas europeias sobre protecção de dados pessoais [6].

Na sua essência, a densificação do conceito de dados sensíveis, assim como as respectivas garantias funcionais e institucionais dos chamados princípios da lealdade, licitude, finalidade e qualidade e que se vertem no direito a ser informado sobre a finalidade, no direito de acesso aos dados, no direito de rectificação ou apagamento, e no direito de oposição como cláusula limite de salvaguarda, importam para o que ora nos interessa.

5. Não nos iludamos: a questão hoje em dia deslocou-se da discussão sobre "o que cabe no âmbito da protecção de que vimos falando" para a necessidade de tutela face a novos meios de violação.

Na verdade, assusta o elenco actual possível de sistemas de telemetria ou de "pegadas electrónicas"que registam e analisam informação telemétrica, biométrica e comportamental: bases de dados de registo de comunicações telefónicas; registo de padrões de comportamento de navegação na Internet; registos de actividade financeira e de transacções comerciais, como movimentos feitos por cartões de débito e de crédito; registos criminais; registos de condução motorizada (deslocação no espaço, velocidade, infracções); registo escolar; arquivos de casos legais; hemerotecas com registos de efemérides no espaço público; registo de obras associadas a propriedade industrial, intelectual e artística; arquivo de imagens de controlo de tráfego; arquivo de imagens de vigilância de espaços públicos; sistemas de reconhecimento de faces; arquivo de impressões digitais; arquivos de identidade; registo de falências; monitorização de comunicação electrónica; registo de redes sociais; registo de compras de fármacos; registo de assinaturas de publicações periódicas; verificação remota da identidade; autenticação contínua; inventário de modos individuais de pressionar as teclas de um teclado; monitorização electrónica da localização de pessoas; etc [7].

---

[6] Em consonância com a obrigatoriedade ditada pela Directiva 95/46/CE, a Lei n.º 67/98, de 25 de Outubro, veio entre nós revogar a Lei n.º 10/91, de 29 de Abril, que pela primeira vez havia regulado entre nós a protecção de dados pessoais.

[7] No geral, sobre as ameaças das novas tecnologias aos direitos fundamentais e a construção de garantias de protecção, leia-se, por exemplo, Seabra Lopes, *A protecção da privacidade e dos dados pessoais na sociedade de informação*, em Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa, pàg.. 779 e seg., Universidade Católica Portuguesa, 2002.

Centremo-nos, para efeitos da análise proposta dos arestos, nestas duas realidades: a facturação detalhada e a recolha de dados de localização e de tráfego possibilitadas pelos novos meios tecnológicos.

II. A ATENÇÃO JURISPRUDENCIAL

II. 1. Acórdão do TC n.º 213/2008 (Processo n.º 671/07, 2.ª Secção)

a) O arguido interpôs recurso da decisão do Tribunal da Relação de Coimbra para o Tribunal Constitucional, ao abrigo do disposto na alínea *b)* do n.º 1 do artigo 70.º da LTC, em que suscitou a inconstitucionalidade das normas contidas nos artigos 125.º e 126.º, n.º 3, e, por extensão do artigo 374.º, n.º 2, "in fine", todos do Código de Processo Penal (C.P.P.), quando interpretadas no sentido de ser permitida a admissão e valoração de provas documentais relativas a dados pessoais do arguido respeitantes à sua vida privada retirados de uma base informatizada, sem o respectivo consentimento, por violação do disposto nos artigos 17.º, 18.º, n.os 1 a 3, 32.º, n.º 8, e 35.º, n.º 4, da CRP.

b) Os dados em questão foram disponibilizados pela empresa "VIA VERDE" para comunicação ao procedimento criminal em causa, a solicitação do Ministério Público, **sem que tivesse sido excepcionado qualquer obstáculo de ordem jurídica, nomeadamente a existência de qualquer sigilo profissional que obstasse ao fornecimento da referida informação.**

O tribunal *a quo* entendeu que qualquer autoridade judiciária, nomeadamente o Ministério Público, podia ordenar a requisição daqueles meios de prova para efeito de junção ao processo e ulterior valoração em sede de julgamento da matéria de facto, desde que o fizesse ao abrigo do disposto no art. 182.º, n.º 1, do C.P.P. e não lhe fosse excepcionado o segredo profissional previsto no artigo 17.º, n.º 1, da Lei n.º 67/98 (doravante L.P.D.P.).

A *ratio decidendi* assumida pelo Tribunal Constitucional centra-se na vinculação resultante da protecção de dados pessoais [8], entendendo essencial o chamado direito à autodeterminação informacional, que se

[8] Este tópico da *ratio decidendi* resulta aqui mais evidenciado do que no Acórdão do TC n.º 486/2009, a referir *infra.*

sobrepõe parcial e garantisticamente ao âmbito de aplicação do direito à reserva da intimidade da vida privada.

De facto, estando em causa o fornecimento de listagem de passagens de um veículo automóvel nas portagens da auto-estrada que foram oportunamente registadas pelo identificador "Via Verde" instalado nesse veículo "e que foram ulteriormente objecto de tratamento informático pela empresa "C., S.A.", no desenvolvimento da relação contratual por esta empresa mantida com o proprietário daquele veículo automóvel", o Tribunal Constitucional não negou a inclusão dos dados em causa no conceito de dados pessoais tal como formulado pela lei portuguesa de protecção de dados (L.P.D.P.), nem questionou que — também nos termos da lei que concretiza o referido artigo 35.º da CRP — o regime restritivo de tratamento e acesso a tais dados se aplica ao que é feito **por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados**.

A justificação desta subsunção resulta evidente do seguinte trecho: "[A]pesar dessa listagem apenas localizar no espaço e no tempo o trânsito de um determinado veículo automóvel, referenciado pela sua matrícula, sendo este necessariamente conduzido por uma pessoa singular, identificável como seu utilizador habitual, essas informações também se lhe reportam, pelo que é correcto dizer-se que estamos perante dados pessoais, nos termos do artigo 3.º, alínea *a)*, da L.P.D.P., sujeitos às regras estabelecidas no artigo 35.º da C.R.P. (este tipo de informações tem sido objecto de tratamento como dados pessoais para efeitos de aplicação da Lei n.º 67/98, de 16 de Outubro, pela Comissão Nacional de Protecção de Dados, como resulta, por exemplo, na autorização n.º 79/2002, ou da deliberação n.º 1/96, acessíveis em www.cnpd.pt)." [(9)]

[(9)] *Ad latere,* o Acórdão desconsidera ainda a circunstância de o veículo automóvel pertencer a uma pessoa colectiva do tipo societário, e o artigo 3.º, alínea *a)*, da L.P.D.P., apenas integrar no conceito de "dados pessoais" os que se referem a pessoas singulares, por entender que a protecção conferida pelo n.º 4 do artigo 35.º da C.R.P. também abrange os dados respeitantes a pessoas colectivas quando deles possa resultar a indicação de dados pessoais concernentes a pessoas singulares, nos casos em que os veículos estão afectos à utilização de uma determinada pessoa em particular, a qual poderá ser identificada — ou identificável — através de outros elementos referenciadores.

c) Não obstante a qualificação *supra* referida, entendeu o Tribunal que "este tipo de dados pessoais, pelas suas características, não se enquadram nos apelidados dados sensíveis (artigo 35.º, n.º 3, da C.R.P.), pertencentes ao núcleo duro dos dados constitucionalmente tutelados, os quais apenas são susceptíveis de tratamento, mediante condições específicas".

Assim, e neste sentido, não aceitou a alegação do recorrente segundo a qual "*sob pena de violação do artigo 18.º, n.º 2, da CRP, será desproporcionado e não conforme com o dito princípio da proporcionalidade, relegar o critério da devassa da vida privada dos cidadãos a entidades que não se encontram imbuídas e submetidas a objectivos e rigorosos critérios deontológicos, com inexistente ou pelo menos insuficiente tutela disciplinar"*.

d) Entendeu o Tribunal que "[A]s listagens em questão apenas permitem, para além do conhecimento da identidade do titular do identificador "via verde", o acesso às "passagens" do veículo automóvel X por determinada portagem de certa auto-estrada, mais concretamente às "horas" e "dias" a que ocorreram essas passagens. (…) A movimentação duma pessoa, nomeadamente a sua deslocação em veículo automóvel, pelas diferentes vias públicas, apesar de ocorrer em locais acessíveis a outras pessoas, é efectuada de forma tendencialmente anónima, pelo que a divulgação de informações sobre essas concretas deslocações automóveis a terceiros (local, dia e hora) poderá comprometer o direito à reserva da intimidade da vida privada do seu condutor. **Mas isso não significa que o acesso a essas listagens, para fins probatórios em processo penal, se traduza numa inadmissível intromissão na vida privada do condutor do veículo em causa".**

O Tribunal Constitucional manteve a decisão recorrida em que o tribunal *a quo* aplicou **o artigo 125.º do C.P.P. de 1987 — na interpretação segundo a qual se permite a admissão e valoração de provas documentais relativas a listagens de passagens de um veículo automóvel nas portagens das auto-estradas, que foram registadas pelo sistema de identificador da "VIA VERDE", armazenadas numa base de dados informatizada e ulteriormente juntas ao processo criminal, sem o consentimento do arguido e por determinação do Ministério Público** — por não entender violado qualquer parâmetro constitucional, nomeadamente o disposto nos artigos 35.º, n.º 4, e 32.º, n.os 4 e 8, da CRP.

e) Não parece que se possa acompanhar, na totalidade, esta decisão do Tribunal. É certo que da ocorrência de determinada situação em vias públicas

decorre certamente uma menor intensidade de tutela, e ainda que "o interesse público constitucionalmente protegido da descoberta da verdade material, essencial à administração da justiça penal como pilar de um Estado de direito, pode justificar a quebra da confidencialidade dos dados pessoais, desde que dela não resulte uma restrição intolerável dos direitos fundamentais do cidadão."

No entanto, e como resulta também de jurisprudência firmada daquele Tribunal, ainda que a prevenção dos crimes constitua uma das competências constitucionalmente reconhecidas às polícias; mas essa competência tem que ser exercida com respeito "pelos direitos, liberdades e garantias dos cidadãos" (cf. artigo 272.º, n.º 3, da Constituição da República). Num Estado de direito democrático «o programa político-criminal deve ser ponderado de modo a garantir o conteúdo essencial dos direitos fundamentais», impostos pela consideração última da dignidade humana.

Ora, parece de entender que a restrição de direitos aqui em causa, ainda que não "intolerável" — para utilizar a expressão do Acórdão — deveria necessariamente passar pelo crivo do especial filtro exigido para os dados sensíveis, mormente o da necessária intervenção de um juíz. De facto, se pode colher o argumento de que a intromissão *sub iudicio* se situa numa "zona já afastada do núcleo mais íntimo da vida privada" para justificar que "prevaleça o interesse superior da obtenção da verdade material na realização da justiça penal, o qual legitima o conhecimento e a valoração probatória judicial das mencionadas listagens" [(10)], já não se acompanha o afastamento da necessária intervenção do juiz garante das posições jurídico-sujectivas dos cidadãos.[(11)]Como veremos, a necessidade de tal intervenção constitui o nó górdio do Acórdão que passaremos agora a explanar.

II. 2. O Acórdão n.º 486/2009 (Processo n.º 4/09, 2.ª secção)

a) Um ano depois, em lugar paralelo para o que nos interessa neste aresto, foi a mesma secção do Tribunal Constitucional confrontado com

---

[(10)] O Acórdão invoca a favor deste passo Paulo Mota Pinto, "*O direito à reserva sobre a intimidade da vida privada*", no BFDUC., vol. LXIX, pág. 566, e *"A protecção da vida privada e a Constituição*", no Boletim da Faculdade de Direito da Universidade de Coimbra, vol. LXXVI, pág. 196, e Maria Fernanda Palma, "*Tutela da vida privada e Processo Penal*", em "Estudos em memória do Conselheiro Luís Nunes de Almeida", pág. 657, Coimbra Editora, 2007.

[(11)] A previsão resulta hoje directamente do n.º 2 do artigo3.º da Lei n.º 32/2008, de 17 de Julho.

recurso interposto ao abrigo do disposto na mesma alínea *b)* do n.º 1 do artigo 70.º da LTC, desta feira referente à **apreciação da constitucionalidade da norma constante do n.º 1 do artigo 187.º do Código de Processo Penal de 1987, na redacção anterior à Lei n.º 48/2007, de 29 de Agosto** [(12)]**, quando interpretada no sentido de que o respectivo conteúdo abrange o acesso à facturação detalhada e à localização celular**.

Invocava o recorrente que tal interpretação normativa se encontrava ferida de inconstitucionalidade material por violação da reserva de lei restritiva de direitos, liberdades e garantias, nomeadamente por permitir a produção e valoração de provas resultantes de intromissões nas telecomunicações não previstas na lei processual penal.

Não obstante analisar a matéria no contexto de alegada "invasão aos direitos fundamentais do cidadão e por isso constitucionalmente protegi-

---

(12) A Lei n.º 48/2007 de 29 de Agosto correspondeu à 15.ª alteração ao Código de Processo Penal, aprovado pelo Decreto-Lei n.º 78/87, de 17 de Fevereiro. Antes dessa data o Código de Processo Penal limitava-se a prever e regular a intercepção e a gravação de conversações ou comunicações telefónicas ou transmitidas por outro meio técnico, aí se compreendendo designadamente e de forma expressa o correio electrónico. Ficavam de fora diligências respeitantes à obtenção de outro tipo de informações, designadamente sobre identificação e morada dos clientes das operadoras de telecomunicações, dados de tráfego e localização celular. Ora, na redacção de 2007, o n.º 1 do artigo 189.º do Código de Processo Penal veio prever que as normas referentes à realização de intercepções telefónicas são correspondentemente aplicáveis "às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital". Por seu turno, o n.º 2 veio determinar a necessidade de autorização do juiz de instrução para a "obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações" e o n.º 3 que caso os dados sobre a localização celular previstos no n.º 1 não se referirem a nenhum processo em curso, a comunicação deve ser dirigida ao juiz da sede da entidade competente para a investigação criminal, e o n.º 4 esclarecia ser nula a obtenção de dados sobre a localização celular com violação do disposto nos números anteriores.

Sobre os meandros e resultados desta alteração processual, leia-se *passim* Manuel Costa Andrade, *"Bruscamente no verão passado", a reforma do Código de Processo Penal — Observações críticas sobre uma lei que podia e devia ter sido diferente*", RLJ, 137.º, 353 e 354, também publicado pela Coimbra Editora em 2009. Em especial sobre vejam-se ainda Benjamim Silva Rodrigues, *A Monitorização de dados pessoais de tráfego nas comunicações electrónicas*, Raízes Jurídicas, Curitiba, v. 3, n. 2, jul./dez. 2007, disponível na Internet e Pedro Verdelho, *A reforma penal portuguesa e o cibercrime*, Revista do Ministério Público, ano 27, n.º 108, Outubro — Dezembro de 2006, pág. 97 e segs., e, do mesmo autor, *Técnica no novo C.P.P.: exames, perícias e prova digital*, Revista do CEJ, n.º 9 (especial), 1.º semestre de 2008, pág. 145 e segs.

dos*"* [13] e de *"*meio de prova que contende com bens jurídicos pessoais que, de forma mais ou menos extensiva e directa, relevam da esfera da privacidade e se caracterizam pela sua estrutura comunicativa e intersubjectiva*"* [14], o *iter* do aresto distingue as situações envolvidas, quais sejam as de:

i) Facturação detalhada;
ii) Localização celular (aqui incluídos em termos gerais dados de localização e tráfego).

i) A '**facturação detalhada***'* surgiu no nosso ordenamento jurídico como um mecanismo vocacionado para a protecção dos utentes de serviços públicos essenciais, nomeadamente, o serviço telefónico [15], decorrente da obrigação — introduzida originariamente pelo artigo 9.º da Lei n.º 23/96, de 26 de Julho, e pelo artigo 1.º do Decreto-Lei n.º 230/96, de 29 de Novembro — do prestador do serviço identificar cada chamada telefónica e o respectivo custo [16].

---

[13] Referia o Parecer de Manuel da Costa Andrade junto aos autos: "[C]omo de todos os lados se acentua — e a própria sentença recorrida não deixa de, expressa e pertinentemente, reconhecer — a facturação e a localização celular configuram atentados específicos à vida privada e, mais directamente, ao sigilo de telecomunicações. E configuram atentados distintos e autónomos face à intercepção e gravação das conversações ou comunicações. Vale por dizer que a sua realização (não consentida) tem de assentar em lei que, de forma específica e autónoma, os legitime. O que, manifestamente, não sucedia na lei processual pena portuguesa vigente até 15 de Setembro de 2007, data a partir da qual, com a entrada em vigor do novo n.º 2 do artigo 190.º, as medidas passaram a gozar de reconhecimento e legitimação legal. Antes disso, nada mais infundado e irreconciliável com a lei e a Constituição do que buscar a legitimação em dispositivos como os artigos 187.º e 188.º do Código de Processo Penal.

Entendimento contrário, isto é, a consideração de que, no silêncio da lei, os meios sempre seriam legítimos porque cobertos pelos artigos 187.º e 188.º do Código de Processo Penal, estaria, pois, irremivelmente ferida de inconstitucionalidade material."

[14] Acórdão do Tribunal da Relação de Coimbra, CJ, 2001, T. II, pág. 44

[15] A introdução da facturação detalhada melhorou as possibilidades de o assinante verificar a exactidão dos montantes cobrados pelo prestador de serviço, embora, possa, ao mesmo tempo, pôr em causa a privacidade dos utilizadores do serviço telefónico pelo conhecimento das "condições factuais das comunicações", como lembra António Pinto Monteiro, "A protecção do consumidor de serviços públicos essenciais", *in Estudos de Direito do Consumidor*, n.º 2, pág. 345-347.

[16] O conceito veio a ser redefinido e burilado pela Lei n.º 41/2004 que tratou como dados de tráfego quaisquer dados tratados para efeitos da facturação do envio de uma comunicação através de uma rede (artigo 2.º, alínea *d)*), como se verá *infra.*

Efectivamente, na definição de factura detalhada incluem-se, pelo menos, informações relativas a todas as chamadas efectuadas num determinado período, aos números de telefone chamados, à data da chamada, à hora de início e à duração de cada chamada, sendo pacífico que a facturação detalhada integra os chamados dados de tráfego relativos às comunicações efectuadas.

A circunstância de serem estes dados essenciais à prestação do serviço de comunicações ao utente, com a necessária obrigação do respectivo registo e armazenagem durante um período de tempo limitado, tem sido invocada para afastar a qualificação como "método oculto de investigação criminal" e a necessidade de consentimento específico no âmbito do processo penal [17]. Esta posição não pode no entanto ser acompanhada sem mais, devendo considerar-se que o tipo de compressão do direito de reserva de vida privada e protecção dos dados pessoais resultante do conhecimento dos "dados de tráfego (facturação detalhada/identificação do n.º chamador)" deve ter a mesma protecção jurídica que os "dados de conteúdo" (intercepção de comunicações electrónicas/escutas telefónicas) e carece de autorização do Juiz de Instrução [18].

---

[17] Sobre este assunto, veja-se Manuel da Costa Andrade, *Métodos ocultos de investigação (Plädoyer para uma teoria geral)*, em Que futuro para o direito processual penal? — Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português", Coimbra Editora, 2009, págs. 534.

[18] Neste sentido, veja-se *v. g.* o Acórdão do Tribunal da Relação de Guimarães, Processo 1341/08.4TAVCT, 12-04-2010:

> *I. Tendo no decurso do inquérito sido participado contra desconhecidos um crime de difamação agravada praticada através da Internet, e visando-se apurar dados de tráfego de comunicações electrónicas (dados relativos às ligações do computador de um agente a um fornecedor de serviço de acesso à Internet), cujo acesso só é possível, nos termos legais, através de autorização do JIC, o regime aplicável é o prevenido no art. 187.º, por remessa do art. 189.º do C.P.Penal. (...)*
>
> *III. E sendo assim, decide-se que deverá o M.º juiz a quo (JIC) solicitar à PT os elementos pretendidos pelo MP.º, após o que, ante uma eventual escusa, haverá de ser accionado mecanismo procedimental previsto no art. 135.º, n.os 2 e 3, do CPP.*
>
> a) *A "identificação dos postos de acesso à Internet", porque "dados de tráfego", "carece de autorização do juiz de Instrução", nos termos do art. 27, n.º 1, al.* g), *da Lei 5/2004, de 10/02 (Lei das Comunicações Electrónicas)*

ii) Por seu turno, a '**localização celular**' — cada vez mais relevante dada a incorporação da tecnologia GPS (*Global Positioning System*) — constitui uma ferramenta mais recente que está associada às redes de telecomunicações móveis: já que constitui condição indispensável para o estabelecimento e transmissão das comunicações, quer durante a fase de arranque da estação móvel, quer quando ocorre uma mudança de área, mas fornece igualmente um grau de precisão muito elevado em matéria de determinação da posição geográfica [(19)].

---

e do art. 4 da Lei 41/2004, de 18/08 (lei do tratamento de dados pessoais e protecção da privacidade no sector as comunicações electrónicas).

b) *Os "dados de tráfego (facturação detalhada/identificação do n.º chamador)" têm a mesma protecção jurídica que os "dados de conteúdo" (intercepção de comunicações electrónicas/escutas telefónicas) "carece de autorização do Juiz de Instrução".*

[(19)] Em sentido que não se pode acompanhar, no Acórdão do Tribunal da Relação de Évora, Processo 2005/08-1, de 07-10-2008, veio determinar-se que "[N]ão carece de prévia autorização judicial o uso pelos órgãos de polícia criminal de localizadores de GPS colocados em veículos utilizados por pessoas investigadas em inquérito (e pelo tempo tido por necessário pelo órgão de polícia criminal encarregue do mesmo", com base na ideia de que a localização por GPS não tem coisa alguma a ver com localização celular", fundando-se na omissão de referência — de regime ou eventual proibição — individualizada da Lei n.º 48/2007, de 29 de Agosto. Entendeu este Acórdão que se deve aplicar o artigo 125.º do CPP que admite as provas não proibidas por lei, já que a utilização de localizadores GPS não consubstancia qualquer dos métodos proibidos de prova a que se refere o art. 126.º

Mas não devia este Acórdão ter desconsiderado quer o n.º 3 do artigo 125.º do CPP quer o n.º 8 do artigo 32.º da CRP, nem podia ter concluído que: "o ter a autoridade policial no decurso de um inquérito criminal acesso à informação de onde está a cada momento um determinado veículo automóvel, não pode ser visto como uma intromissão na vida privada de quem vai nesse veículo, pois que o GPS é um aparelho surdo e cego no sentido de que não escuta as conversas dos ocupantes do carro, nem identifica quem lá vai e o que estão a fazer, apenas informa aonde está o veículo, circunstância que é visível a olho nu para quem olhe para o carro e lhe vê a matrícula. Daí que expressões ou divulgações como: «estava lá o carro de Fulano», «vi passar o carro de Sicrano» ou «o carro de Beltrano fica todas as noites estacionado à porta da Maria», não constituam qualquer comportamento tipificado como crime de devassa da vida privada". Parece-nos gravoso aceitar-se que "a localização por GPS é o «irmão gémeo electrónico» do clássico seguimento do alvo por pessoas a bordo de um carro", sem distinguir o grau de intrusão que um e outro permitem e que desde logo radica na previamente distintiva necessidade de uma prévia suspeição de actividade ilícita. Aliás, esta circunstância foi objecto de censura no Parecer n.º 10/2003 da Comissão Nacional de Protecção de Dados, a que se fará referência *infra.*

Os dados de localização podem, assim, incidir sobre a latitude, a longitude e a altitude do equipamento terminal do utilizador, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização [20].

Como refere o Acórdão *sub judice,* aqui chegados, importa, portanto, concluir que os dados da facturação detalhada e os dados da localização celular que fornecem a posição geográfica do equipamento móvel, na medida em que são tratados para permitir a transmissão das comunicações, se **encontram abrangidos pela protecção constitucional conferida ao sigilo das telecomunicações.**

Questão diversa será a da discussão quanto ao diferente grau de ofensa que o acesso a estes dados reveste para os direitos e liberdades protegidos pelo sigilo das telecomunicações, relativamente às "escutas telefónicas", "quer pela menor informação que revelam, quer pelo facto de não se tratar de um método oculto de obtenção de prova, o que tem suscitado a interrogação sobre se esse acesso deve estar sujeito aos mesmíssimos pressupostos." [21]. Aliás, diga-se que a eventual diferente natureza da invasão nada depõe relativamente à respectiva intensidade, já que *"***aceder à intensidade dos contactos com determinado posto telefónico constitui uma verdadeira intromissão na intimidade dos cidadãos visados***"*. Por outro lado*, "***o acesso à localização celular é indiscutivelmente uma intromissão penetrante na esfera da privacidade e intimidade do cidadão. Este meio representa um autêntico controlo à distância do cidadão facultando acesso a todos os seus movimentos***"*.

b) O Tribunal começou por se ocupar da questão orgânica, ou seja, a de saber se podia ou não concluir-se pela verificação de violação do prin-

---

[20] Em conformidade com a Directiva n.º 2002/58/CE, a Lei n.º 41/2004 considera os dados de localização que fornecem a posição geográfica do equipamento terminal como dados de tráfego apenas na medida em que sejam estritamente tratados pela rede móvel para permitir a transmissão de comunicações, ficando fora desta classificação os dados de localização que são mais precisos do que o necessário para a transmissão das comunicações e que são utilizados para a prestação de serviços de valor acrescentado, tais como serviços que prestam aos condutores informações e orientações individualizadas sobre o tráfego (artigos 2.º, alíneas *d)*, *e)* e *f)*, 6.º e 7.º).

[21] Sobre este passo do Acórdão, veja-se Mouraz Lopes, *Escutas telefónicas: seis teses e uma conclusão*, R.M.P., Ano 26.º, n.º 104, págs. 143.

cípio da legalidade no âmbito do processo penal, por referência ao inciso que resulta do n.º 4 do artigo 34.º da CRP que proíbe *"toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal."*

A discussão quanto ao âmbito de previsão da expressão *"nos casos previstos na lei"* para efeitos da consideração da '*reserva de lei'* e *'preferência de lei'*, não se apartou do conhecimento das posições divergentes sobre se a fiscalização do princípio da legalidade, designadamente em matéria fiscal e penal, se insere nas atribuições do Tribunal Constitucional, nos termos e para efeitos do n.º 3 do artigo 80.º da LTC.

E o Tribunal conclui, acertadamente — e na linha do Acórdão do TC n.º 183/2008 — que quando o "referente da norma em causa é uma realidade típica com um elevado grau de abstracção, como sucede com o "acesso à facturação detalhada" e a "localização celular", as quais se mostram, aliás, parcialmente configuradas pelo legislador europeu e nacional (vide a Lei n.º 41/2004, de 18 de Agosto), os argumentos fundamentais invocados para não conhecer das eventuais violações do princípio da legalidade deixam de ter apoio".

Ora, nesta senda, encontrando-se o acesso à facturação detalhada e a localização celular compreendidas no real conteúdo das técnicas de ingerência nas telecomunicações expressamente previstas pelo legislador no artigo 187.º do C.P.P./87, não considerou o Tribunal que a interpretação normativa sindicada desrespeite o princípio da legalidade consagrado no n.º 4 do artigo 34.º da C.R.P., pelo que entendeu o recurso improcedente com base neste fundamento [(22)].

c) Mas o Tribunal discutiu ainda, as hipóteses de restrição e ingerência na contextualização da expressão utilizada pelo legislador ordinário no n.º 1 do artigo 187.º do CPP (na redacção da época) sobre a intercepção e a gravação de conversações ou comunicações telefónicas, porquanto intromissões e ingerências nas telecomunicações só poderão ser acolhidas no nosso ordenamento desde que respeitem o regime das restrições de

---

[(22)] Sobre esta matéria a Lei n.º 41/2004, conforme já ficou dito, limita-se a admitir as excepções à sua aplicação que se mostrem necessárias «para a prevenção, investigação e repressão de infracções penais», «definidas em lei especial» (artigo 1.º, n.º 4), a qual nesse contexto é o Código de Processo Penal.

direitos liberdades e garantias estabelecido nos n.os 2 e 3 do artigo 18.º da Constituição, e com a acrescida exigência do n.º 4 do artigo 34.º e do n.º 8 do artigo 32.º da CRP que dispõe que*"[S]ão nulas todas as provas obtidas mediante (...) abusiva intromissão (...) nas telecomunicações"*.

d) Sem nos restringirmos às previsões normativas do CPP em vigor à data da prolação do Acórdão n.º 486/2009, e neste contexto de alusão ao regime de métodos de prova, torna-se necessário dilucidar os conceitos que decorrem da análise do historial — ainda que anterior ou ulterior — dos diplomas legislativos que começaram a regular a matéria dos dados de base, dados de tráfego e dados de conteúdo: esta tripartição dos dados envolvidos no serviço de telecomunicações foi consolidada pelo Conselho Consultivo da Procuradoria-Geral da República nos Pareceres n.º 16/94 — acessível em www.dgsi.pt — e Parecer n.º 21/2000, publicado no DR II Série, de 23 de Julho de 2002.

De harmonia com esses Pareceres, no serviço de telecomunicações podem distinguir-se as seguintes espécies de dados:

i) *dados relativos à conexão à rede, ditos dados de base, que nos termos da 4a conclusão do Parecer n.º 16/94, da PGR, são os relativos ao posto e ao número de acesso;*
ii) *os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego;*
iii) *e os dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo.*

Os mesmos Pareceres recortavam ainda quatro momentos essenciais dos vários serviços de telecomunicações utilizados para a transmissão de comunicações verbais ou de outro tipo (mensagens escritas [23], dados por

---

[23] No que respeita ao serviço de mensagens curtas (SMS) e o serviço de mensagens multimédia (MMS), os dados de conteúdo, como sejam o teor das mensagens só podem ser objecto de intercepção em tempo real, com a devida autorização judicial, não tendo cabimento pedir às operadoras de rede móvel que operam em Portugal a remessa em suporte digital (cd ou dvd) dos conteúdos de comunicações e mensagens expedidas e recebidas entre determinados telefones, num determinado período do passado, dada a

pacotes): a fase prévia à comunicação, o estabelecimento da comunicação, a fase da comunicação propriamente dita e a fase posterior à comunicação.

No primeiro tempo relevam essencialmente os dados de base, enquanto que nos restantes importa essencialmente a consideração dos dados de tráfego e de conteúdo.

i) Como acentuam os Pareceres referidos, na perspectiva dos utilizadores, dados de base são os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respectivo serviço: *v. g.,* nome, morada, e os dados que aquela empresa fornece, em sentido inverso, ao utilizador para efeito de interligação à rede e ou ao serviço de comunicações electrónicas, *v. g.,* número de acesso, nome de utilizador, password.

ii) Os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, é operada ou transmitida, são a direcção, o destino (adressage) e a via, o trajecto (routage). Estes elementos funcionalmente necessários ao estabelecimento e à direcção da comu-

---

impossibilidade legal de os dados de conteúdo das mensagens e ou comunicações, se estas existiram, terem sido objecto de registo e gravação. É que estes só podem ser obtidos através da colocação prévia de meios técnicos de intercepção e gravação do conteúdo das mensagens em causa, o que sempre careceria de avaliação da sua legalidade pelo juiz de instrução, quer em termos de admissibilidade, quer em termos de necessidade, adequação e proporcionalidade.

Quanto ao conteúdo de SMS e MMS, veja-se a propósito o Acórdão do Tribunal da Relação de Évora n.º 111/08-1, de 29-04-2008, que determina que "[N]ão há razão para distinguir (…) entre os dois tipos de comunicações — conteúdo de mensagens SMS e MMS e listagens do tráfego telefónico referente às chamadas recebidas e efectuadas. Onde a lei não distingue, a ninguém é dado distinguir". E, numa conclusão que não pode acompanhar-se:"[O] direito à reserva da intimidade da vida privada não corre maior risco de ser lesado pelo acesso ao conteúdo de mensagens SMS ou de MMS do que pelo conhecimento das precisas circunstâncias de tempo, lugar, modo e frequência das chamadas recebidas e efectuadas".

No mesmo sentido, que igualmente se censura, veja-se o Acórdão do Tribunal da Relação do Porto, Processo 1978/09.4JAPRT-B.P1, de 07-07-2010: "A informação guardada no cartão SIM de um telemóvel e relativa a conversações ou mensagens — SMS — expedidas ou recebidas, mesmo que não lidas pelo seu detentor, não pertence à área de tutela das telecomunicações, constituindo um normal escrito e podendo, como tal, ser objecto de apreensão, através da apreensão do telemóvel e do cartão SIM. II — O facto daqueles dados caírem fora da tutela do sigilo das telecomunicações não os torna dados livres e expostos à devassa e rapacidade: **não sendo exigível a intervenção do juiz na apreensão já tal intervenção se torna exigível na permissão de acesso aos dados**".

nicação identificam, ou permitem identificar a comunicação: quando conservados, possibilitam a identificação das comunicações entre o eminente e o destinatário, *v. g.,* data e hora do início da sessão (login) e do fim (logoff) da ligação ao serviço de acesso à Internet, endereço de IP atribuído pelo operador, volume de dados transmitidos, entre outros.

Constituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento directo entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações.

iii) Finalmente, os elementos de conteúdo — dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede." [(24)].

Aplicando estes conceitos, dir-se-á, acompanhando a explanação oferecida pelos Pareceres *supra* referidos: "suponhamos que António celebra um contrato com um ISP para o fornecimento de acesso à Internet e cede o que designamos por dados de base. Já na posse de todos os elementos necessários para a ligação à Internet, envia uma mensagem de correio electrónico a um colega, com o seguinte conteúdo: "Convite para jantar amanhã às 17h00. Abraço. António". A hora de envio, o volume de dados transmitidos, o IP de origem, entre outros configuram o que apelidamos de dados de tráfego, e, por último, a mensagem enviada integra-se no conceito de dados de conteúdo".

Dispunha o diploma que entre nós veio inicialmente regular o tratamento dos dados pessoais e a protecção da privacidade no sector das telecomunicações, a Lei n.º 69/98, de 28 de Outubro — que transpunha e acompanhava o conteúdo da Directiva 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, especificando e complementando as disposições da Lei n.º 67/98, de 26 de Outubro (LPDP). Determinava que os dados de tráfego deviam ser apagados ou tornados anónimos após a conclusão da chamada (n.º 1 do artigo 6.º), sem prejuízo da possibilidade de tratamento de dados relativos à facturação dos serviços prestados até final

---

[(24)] 4. Em relação ao acesso a *dados de conteúdo* não há qualquer objecção uma vez que, no contexto do artigo 34.º, n.º 4, da CRP e com referência ao artigo 187.º do CPP, essa diligência é ordenada ou autorizada por despacho do juiz, devendo obedecer às formalidades do artigo 188.º

do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado (n.º 3 do mesmo artigo), ou do seu tratamento com o consentimento do assinante para outras finalidades determinadas (n.º 4).

Entretanto, com a evolução das directivas comunitárias em matéria de comunicações electrónicas verificou-se uma metamorfose no paradigma da protecção jurídica dos dados pessoais em que, ao lado da mencionada trilogia de dados de tráfego, de base e de conteúdo, surge a definição de dados de localização De facto, a introdução de novas tecnologias digitais nas redes de comunicações públicas determinou a necessidade de acautelar novos requisitos específicos de protecção de dados pessoais e da privacidade dos utilizadores, o que se traduziu na adaptação e revogação da Directiva n.º 97/66/CE pela Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho. E, assim, mercê do dever de transposição desta nova directiva europeia, a referida Lei n.º 69/98 foi revogada pela Lei n.º 41/2004, de 18 de Agosto, a qual veio aprovar o regime jurídico do tratamento de dados pessoais e da protecção da privacidade no sector das comunicações electrónicas [(25)].

No entanto, importa lembrar que a matéria havia já sido objecto de tentativa de tratamento no nosso ordenamento jurídico: de facto, a Comissão de Protecção de Dados havia já analisado a questão a pretexto da apresentação do Projecto de Lei n.º 217/IX ('Regime Jurídico da Obtenção da prova digital na Internet') [(26)] pelo Grupo Parlamentar do Partido Popular, tendo então prolatado o seu Parecer n.º 10/2003 (Proc. 366/03) [(27)].

[(25)] Os dados de localização estão estreitamente relacionados com os dados de tráfego na medida em que a localização diz respeito ao equipamento terminal de um utilizador do equipamento previamente identificado. São dados de localização «quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um assinante ou de qualquer utilizador de um serviço de comunicações electrónicas acessível ao público» na definição da alínea *e)* do n.º 1 do artigo 2.º da Lei n.º 41/2004. Estes dados são tratados nas redes móveis digitais para possibilitar a transmissão das comunicações mas tornam praticável a chamada localização celular, através da qual se pode conhecer em que local se encontra o detentor de um telefone móvel e a sua movimentação. Nessa medida são dados pessoais e o regime regra é o de que o respectivo tratamento é apenas permitido se os dados forem tornados anónimos (artigo 7.º, n.º 1, da Lei n.º 41/2004).

[(26)] Veja-se, por todos, Pedro Verdelho, *Técnica do Novo CPP: Exames, Perícias e Prova Digital*, Revista do CEJ, 1.º semestre de 2008, n.º 9, pág. 164.

[(27)] Acrescente-se ainda que a Comissão já analisara questão homotética na sua Deliberação n.º 29/98, de 16 de Abril, muito em consonância com o Parecer da PGR n.º 16/94, de 2.5.96.

O referido parecer era por demais violento e virulento, ainda que justificado pelos termos incipientes e sem densificação em que a referida iniciativa era apresentada. De acordo com o que se adiantava na respectiva 'Exposição de Motivos', o Projecto tinha em vista garantir "o acesso urgente, por parte das autoridades à informação necessária e suficiente para a investigação criminal, proporcionando-lhes a forma de acederem, em tempo útil, à informação disponível nas operadoras de comunicações que permita a identificação dos autores e o registo dos actos ilícitos praticados através dos meios informáticos e de comunicações".

Como bem veio referir a Comissão Nacional de Protecção de Dados, o projecto de lei reflectia a "tendência internacional de produção de nova legislação de cariz securitário, em grande parte explicada pelos trágicos acontecimentos de 11 de Setembro de 2001" bem como a "preocupação com novas formas de criminalidade, ou com velhas formas de criminalidade praticadas com a utilização de novos métodos" que dita a regulação da cyber-criminalidade [(28)].

A Comissão Nacional de Protecção de Dados concluía que: "[À] perigosa fúria legislativa ameaçadora da privacidade dos cidadãos parece não querer escapar, ainda que de forma mais tímida, o legislador português, e outros legisladores europeus" mas avisava que lhe cabia controlar "se os instrumentos utilizados com intuito securitário impõem ameaças intoleráveis à privacidade".

Cotejando o projecto de lei com as regras internacionais aplicáveis, aaquela autoridade administrativa enveredava por censuras várias, que se elencam sumariamente:

i) No geral, o desrespeito pela Recomendação do Conselho da Europa sobre a protecção dos dados pessoais no sector das telecomunicações, que determinava:

> *"4.2. Os dados pessoais recolhidos e tratados pelos operadores de rede ou prestadores de serviços podem ser comunicados às*

[(28)] Nesse contexto, veio a ser publicada a Lei n.º 109/2009, de 15 de Setembro, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

autoridades públicas se esta comunicação for prevista pela lei e constituir uma ***medida necessária, numa sociedade democrática****:*

a) *à protecção da segurança do Estado, à segurança pública, aos interesses monetários do Estados ou à repressão de infracções penais;*
b) *à protecção da pessoa em causa e dos direitos e liberdades de outrem.*

4.3. No caso de comunicação de dados pessoais às autoridades públicas, ***o direito interno deveria regulamentar:***

a) ***o exercício dos direitos de acesso e de rectificação pela pessoa em causa;***
b) ***as condições em que as autoridades públicas competentes terão o direito de recusar dar informações à*** *pessoa em causa ou de adiar a entre a das mesmas;*
c) ***a conservação ou a destruição destes dados".***

ii) A preocupação com os "excessos securitários que se pretende impor de forma a vigiar, por antecipação e de forma generalizada, todos os cidadãos", entendendo a Comissão Nacional de Protecção de Dados que importava "contrariar a actividade legislativa sob a pressão dos acontecimentos do 11 de Setembro, que restringem liberdades e direitos fundamentais";

iii) Inexistência de "necessidade social imperativa que justifique estas medidas que se pretende aplicar por tempo indeterminado, a todas as pessoas e, em alguns casos, independentemente das circunstâncias";

iv) A circunstância de o dever de comunicação não depender de autorização judicial — prévia, ou posteriormente confirmada — podendo, inclusivamente, ser exercido para efeitos de prevenção criminal e não apenas para efeitos de investigação criminal (sendo que ao contrário da investigação criminal, a prevenção não depende do controlo das autoridades judiciárias, pelo que seriam acrescidos os riscos que poderão daí resultar) [(29)];

[(29)] No Parecer do Conselho Consultivo da PGR n.º 21/2000, entendeu-se que os dados de tráfego só poderiam ser fornecidos pelos operadores de telecomunicações nos termos aplicáveis à intercepção de comunicações.

Também se tomou posição sobre os "dados de base", entendendo que se encontram

v) A permissão do acesso a dados pessoais, sem autorização judicial, sem necessidade de existência de um processo ou de uma suspeita, tendo como única condição que o cidadão não tenha, previamente, manifestado de forma expressa o desejo de não serem publicitados os seus dados, havendo aqui violação do princípio do consentimento e da finalidade do tratamento de dados pessoais.

Neste sentido, o Parecer n.º 10/2003 da CNPD veio concluir pela ausência de sentido da distinção que a jurisprudência fazia entre dados de base, de tráfego e de conteúdo, pois que tudo se trata de comunicações, a merecer o mesmo tratamento jurídico, uma vez que ao solicitar-se a facturação detalhada de um determinado telefone está-se a por em causa a privacidade dos utilizadores de chamadas, os quais podem nada ter a ver com o arguido.

Subsequentemente, em Parecer n.º 27/2004 sobre a mesma matéria, que incidiu sobre o Registo 38/Prop/2004 ('Proposta de Lei que define o

---

cobertos pela regra da confidencialidade, nesse caso de génese privatística ou contratual, a qual «releva de um simples interesse pessoal do utilizador que não contende com a sua esfera pessoal íntima» e entendeu-se nessa conformidade que «poderão ser comunicados, a pedido de qualquer autoridade judiciária, para fins de instrução criminal, em ordem ao prevalecente dever da colaboração com a administração da justiça» (conclusão 3.ª). Em sentido contrário, no Parecer n.º 16/94 tinha sido entendido que estariam submetidos às mesmas garantias que os elementos da comunicação propriamente dita e dessa forma abrangidos pelo regime do artigo 269.º do Código de Processo Penal.

Do exposto, resulta que o actual quadro legal confere aos dados de tráfego (facturação detalhada/identificação do número chamador) igual protecção jurídica que na vigência da Legislação ora renovada (Lei n.º 91/97, de 1 de Agosto, e Lei 69/98, de 28 de Outubro) era cometida apenas aos dados de conteúdo (intercepção das comunicações electrónicas/escutas telefónicas). Ou seja, a inviolabilidade das comunicações electrónicas abrange, actualmente, não só as comunicações (dados de conteúdo) mas também, os respectivos dados de tráfego, razão pela qual o seu fornecimento carece de autorização do Juiz de Instrução.

O legislador veio, deste modo, consagrar no artigo 4.º da Lei n.º 41/2004, de 18 de Agosto, a doutrina vertida no Parecer n.º 21/2000, do Conselho Consultivo da PGR que, na conclusão 2.ª, prescreve o seguinte:

> "Na fase de inquérito, tais elementos de informação, quando atinentes a dados de tráfego ou a dados de conteúdo, apenas poderão ser fornecidos às autoridades judiciárias, pelos operadores de telecomunicações, nos termos e pelo modo em que a lei de processo penal permite a intercepção das comunicações, dependendo de ordem ou autorização do Juiz de Instrução (artigos 187.º, 190.º e 269.º, n.º 1 alínea *c)*, do Código de Processo Penal."

regime de prova digital electrónica*')* do XV Governo Constitucional, a Comissão Nacional de Protecção de Dados levantou uma vez mais dúvidas várias de compatibilização com o acervo constitucional e legal em vigor — em especial com a Lei n.º 69/98, de 28 de Outubro — reiterando que a "reserva em relação a estes dados visa assegurar uma certa tranquilidade dos interessados contra intromissões possibilitadas ou potenciadas pela divulgação pública de tais elementos".

A Comissão veio assumir a distinção entre a natureza contratual da "obrigação de confidencialidade" (dever geral de segredo profissional) para os agentes dos operadores das redes públicas e de serviços de telecomunicações quando o assinante assim o pretende e a protecção conferida aos dados de tráfego (*v. g.* duração da utilização, data, hora e frequência) e de conteúdo da comunicação, que beneficiam de protecção constitucional e integram, em bom rigor, o núcleo de informação protegido pelo sigilo das telecomunicações (cf. artigo 34.º, n.os 1 e 4, da CRP).

No que tange a este Parecer n.º 27/2004, a Comissão veio acentuar:

a) a incorrecta transposição das definições resultantes da Directiva 2002/58/CE, em especial no que tange ao conceito de dados de tráfego e ao conceito de dados de base, já que ao serem incluídas na definição de «dados de base» as informações relativas à «*listagem de movimentos de comunicações* », corre-se o risco de confusão pois os «dados de tráfego» podem abranger a mesma realidade (ou realidades similares) na medida em que englobam a "origem da comunicação, o destino e os trajectos»;
b) a persistência das críticas resultantes do Parecer n.º 10/2003 relativamente à necessidade, obrigatoriedade de conservação e acesso aos dados relativos aos dados de localização, de tráfego e de base e ainda relativamente ao acesso a dados de conteúdo;
c) a contradição com as regras resultantes da Convenção do Conselho da Europa sobre Cibercriminalidade, de 23/11/2001.

Nova versão feita circular entretanto pela Ministra da Justiça do XV Governo Constitucional veio a resultar na emissão do Parecer n.º 29/2004 da mesma Comissão, desta feita favorável por entender que se tinham feito as alterações consideradas necessárias e pertinentes no sentido de limitar o acesso pela Polícia Judiciária a dados que estejam sujeitos ao regime de confidencialidade ou que envolvam o sigilo das telecomunicações. Em especial, nesta fase final estava em causa a necessidade de fazer depender

o acesso às "listas de movimentos de comunicações" de despacho fundamentado de autoridade judiciária titular da direcção do processo. Torna-se assim claro que o acesso à chamada facturação detalhada está dependente de despacho de autoridade judiciária, assim se coadunando com a tutela constitucional do sigilo da correspondência e das telecomunicações.

e) A referida Lei n.º 41/2004, aliás tal como a Directiva que transpõe, é um diploma sobre tratamento de dados pessoais e protecção da privacidade que, no contexto da disciplina da segurança e confidencialidade das comunicações, regula o aspecto parcelar do destino final dos dados de tráfego que foram necessários para a transmissão da comunicação.

A evolução normativa até à presente data conclui-se com a Lei n.º 32/2008 [(30)], de 17 de Julho, que transpõe para a ordem jurídica interna

---

[(30)] Em conformidade com a directiva europeia transposta, a Lei n.º 41/2004 não prejudica a possibilidade de existência de legislação especial que restrinja a sua aplicação no que respeita à inviolabilidade das comunicações, nomeadamente para efeito de investigação e repressão de infracções penais (artigo 1.º, n.º 4).

A Lei n.º 32/2008 pode ser entendida como lei especial em relação à Lei n.º 41/2004, relativamente à qual introduz aditamentos e estabelece derrogações no que respeita à conservação e transmissão para determinadas finalidades de dados gerados ou tratados no contexto das comunicações electrónicas. Mas também é muito claro, quanto a ela, que tem em vista dados em suporte electrónico. Com efeito, o objectivo que legitima a conservação dos dados é precisamente o de facultar a sua transmissão imediata, «mediante despacho do juiz, às autoridades competentes» (alínea *a)* do n.º 1 do artigo 7.º). Essa transmissão far-se-á mediante comunicação electrónica, rodeada das medidas que assegurem a sua inviolabilidade referidas no n.º 3 do mesmo artigo 7.º, sem intervenção portanto de suportes em papel. Constata-se assim do que antecede que tanto a Lei n.º 41/2004 como a Lei n.º 32/2008 têm em vista informações em suporte electrónico e apura-se, em consequência, que o regime de conservação e armazenamento previsto e regulado pelas Leis n.º 41/2004 e n.º 32/2008 não é aplicável a documentos em papel que contenham ou reproduzam, na terminologia da consulta, "informação confidencial", "informação confidencial dos clientes", "dados pessoais e de tráfego", ou informações sobre comunicações que foram objecto de intercepção, dados estes todos anteriormente gerados e tratados por via electrónica.

No sentido de acentuar estas conclusões, veja-se o Parecer do Conselho Consultivo da PGR de 07.05.2009, publicado no DR em 02-10-2009, em que são expendidas as seguintes conclusões:

> 1.ª Aos dados de tráfego, dados de localização, registos de comunicações, registos de chamadas interceptadas e informações sobre o nome, morada e número de assinante que não figurem em listas de assinantes, inscritos em suporte de papel e estruturados em ficheiros, que sejam produto do tratamento de dados constantes de suporte electrónico com a finalidade de serem transmitidos aos órgãos de polí-

a Directiva n.º 2006/24/CE, de 15 de Março de 2006, em cuja elaboração esteve presente a memória dos ataques terroristas ocorridos em Londres em 2005 e foi evocada «a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações». A Lei n.º 32/2008 tem um âmbito mais restrito porque incide em primeira linha sobre o destino e transmissão dos dados de tráfego e de localização, desenvolvendo a disciplina legal anterior e consagrando soluções novas [31].

f) De tudo o que fica dito resulta evidente a dupla função do tipo de dados a que nos vimos referindo. De facto, a chamada facturação detalhada é um meio colocado ao dispor do assinante para verificar a exactidão dos

---

cia criminal e autoridades judiciárias, aplica-se o regime de tratamento dos dados pessoais estabelecido pela Lei n.º 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais;

2.ª Os dados, registos e informações inscritos em suporte de papel, mencionados na conclusão anterior, não deverão ser conservados pelas empresas operadoras para além do período necessário para a sua transmissão às entidades referidas;

3.ª Às empresas operadoras de telecomunicações não é exigido qualquer juízo sobre a relevância das vicissitudes do processo penal em curso quanto à pertinência ou necessidade de conservação dos referidos elementos."

[31] O n.º 2 do artigo 1.º da Lei n.º 32/2008, de 17 de Julho vem determinar que "[À] conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à intercepção e gravação de comunicações", adoptando as definições constantes das Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto.

Acentua-se que a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes e que só pode ser ordenada ou autorizada por despacho fundamentado do juiz, não podendo o titular dos dados não pode opor-se à respectiva conservação e transmissão (n.os 2 e 4 do artigo 3.º).

O diploma identifica ainda (n.º 1 do artigo 4.º) as categorias de dados a conservar:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
b) Dados necessários para encontrar e identificar o destino de uma comunicação;
c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d) Dados necessários para identificar o tipo de comunicação;
e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

Finalmente, são ainda especificadas no artigo 11.º as condições de destruição dos dados.

montantes cobrados pelo prestador do serviço mas, sendo um registo de conversações telefónicas, e, consequentemente, de dados de tráfego, põe em causa a privacidade dos utilizadores das comunicações electrónicas. Certamente por essa razão o artigo 8.º da Lei n.º 41/2004 admite a regulação da matéria com intervenção da Comissão Nacional de Protecção de Dados.

Em especial no que respeita à obrigatoriedade de conservação e/ou destruição, e como acentuava o Parecer de 2009 do Conselho Consultivo da PGR, da descrição dos regimes dos dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas à luz do regime da Lei n.º 41/2004, e do regime especial da Lei n.º 32/2008, "não fica claro se aqueles documentos deverão ser encarados como expressão directa de comunicações electrónicas, e a esse título submetidos ao regime das duas leis acabadas de indicar, ou como produto acessório ou lateral dessas comunicações e meros sucedâneos de existentes suportes electrónicos, destes podendo ou devendo ser separados e ser objecto de consideração diferenciada, em termos tais que a esses documentos caiba aplicar outro regime. A vingar o primeiro termo da alternativa, que insere os dados em causa no âmbito da comunicação electrónica, o princípio geral aplicável no quadro da vigente Lei n.º 41/2004 não é o de estabelecer uma permissão; tem antes o sentido contrário de estabelecer um dever ou imposição — os dados, os documentos em papel entendidos como expressão ou manifestação desses dados, «devem» ser eliminados ou tornados anónimos «quando deixem de ser necessários para efeitos da transmissão da comunicação» conforme se dispõe no n.º 1 do artigo 6.º da Lei n.º 41/2004 Mas "podem" manter-se armazenados para determinados efeitos, designadamente facturação, pagamento de interligações e, com o consentimento do assinante ou utilizador, para prestação de determinados serviços, todavia sempre por tempo limitado (n.os 2 a 5 do artigo 6.º da Lei n.º 41/2004). Esgotado este, revive a obrigatoriedade do apagamento ou de anonimato".

g) Feito este excurso e aventada a questão do grau de intrusão no que tange ao direito probatório, parece não proceder por si o pressuposto de que a escuta de uma comunicação é mais invasiva que o acesso aos dados de tráfego ou/e à localização celular. Muitas vezes uma comunicação não evidência mais que um dialogo de conteúdo inócuo — seja porque os interlocutores não o pretendem fazer ao telefone —, mas a circunstância de se aceder ao número de vezes que se liga para determinado aparelho já pode ter um conteúdo forte e o acesso à localização celular é em si mesmo profundamente invasivo do direito à privacidade.

Raciocínio diferente — e exactamente oposto — é o que de sendo esses dados de tráfego apenas uma parte dos dados facultados pela realização de "escutas telefónicas", nada obstará, e até imporá a exigência que as técnicas de intromissão nas comunicações telefónicas se limitem à medida necessária para alcançar o objectivo de investigação criminal visado, que o acesso a esses dados de tráfego seja efectuado, dispensando a realização duma "escuta telefónica", quando esta não se revele necessária aos fins da investigação. No mesmo sentido, saber a "localização celular" tem o mesmo intuito probatório e a mesma eficácia de uma vigilância tradicional efectuada por agentes policiais sobre determinado indivíduo, ainda que esta última possa ser mais intrusiva (no sentido de permitir a quem a efectua recolher muito mais informação, designadamente sobre a privacidade da pessoa vigiada) que a dita "localização celular". (32)

III. QUID JURIS?

1. Importa terminar. Pergunte-se, em jeito de conclusão, como compaginar o direito à privacidade, com os assentimentos dados pelo TC ou com o facto de, por exemplo, toda a Oxford Street londrina estar milimetricamente coberta por câmaras, o mesmo sucedendo em algumas cidades espanholas, aliás com a chancela expressa do Tribunal Constitucional do país vizinho? Estará a solução numa ficção de consentimento, em virtude do bem comum da segurança?

São estas as questões que nos devem ocupar, hoje em dia. Há quem já tenha defendido que não são questões novas — tratar-se-ia, numa conhecida expressão a lembrar o responsável máximo pela organização destas jornadas, de mero "vinho novo em odres velhos"— mas há outros que reclamam com veemência novas regras e não um mero *update* das existentes.

Mais uma vez — e ainda que os objectivos possam ser respeitáveis —, assistimos à emergência de um mundo onde é provável que ninguém, num

---

(32) Por isso, é acentuado *"*o significado da consciência de não se estar a ser secretamente vigiado como garante de uma utilização activa dos direitos humanos através dos cidadãos e como elemento central de uma democracia que funciona*",* Hans-Jorg Albrecht, *Vigilância das telecomunicações. Análise teórica e empírica da sua implementação e efeitos*, Que Futuro Para o Direito Processual Penal? — Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português, da Coimbra Editora, 2009, págs. 728.

futuro próximo, possa vir a ser deixado em paz. Há quem diga, por isso, que a vida privada pelo menos como foi concebida na modernidade, é um conceito em vias de extinção.

2. Dependendo desde logo a economia e a segurança tão fortemente da informação — e sobretudo da informação personalizada que permita a actuação de forma cada vez mais precisa — a violação da privacidade individual irá necessariamente intensificar-se. Ora, isto tornará a privacidade um bem raro, algo de precioso, cuja valorização crescerá exponencialmente. O ataque ao único não resulta afinal da destruição do individual mas da sua apropriação. A "morte da privacidade" deve, assim, ser reinventada para reclamar antes a transparência dos procedimentos de restrição de direitos, num modelo sempre centrado no teste triplo da proporcionalidade — necessidade, adequação e proibição do excesso —, que parece simplista, mas que é, ao invés, exigente e clarificador.

3. É certo que a chamada teoria das bagatelas — como princípio de interpretação e conformação — exclui a protecção típica quando entende não existir adequação social: neste sentido, importa que percebamos que o âmbito de protecção do direito à reserva da vida privada exige, no mundo actual, uma configuração obviamente distinta daquela a que se referia Brandeis no final do século XIX. Mas tal constatação não pode olvidar a vinculação do legislador ordinário e do intérprete julgados aos direitos fundamentais.

E, neste contexto, não se deixe de louvar a preocupação pedagógica e formadora formulada em 2004 pela CNPD quanto à instalação de câmaras numa creche, no que tal representaria de sinal dado num Estado de Direito Democrático: a captação de imagens solicitada poderia criar nas crianças, no entendimento da Comissão "a habituação ou aceitação natural da sujeição a tal modo de controlo, na sua vida futura."

Se a privacidade está destinada a ser algo de apenas residual e se aquilo que nos espera é, de forma inevitável, um mundo "transparente", então o verdadeiro desafio que se coloca hoje não é o de reclamar novos instrumentos que sejam capazes de nos devolver alguma da privacidade perdida mas sim o de exigir mais transparência e legitimação procedimental. Numa conclusão que nada tem também de novo, o essencial é desenvolver formas institucionais de "poder ver aqueles que nos vêem". Talvez seja esse o garante da viabilidade, ainda hoje, do tal direito a "ser deixado em paz."