



DELIBERAÇÃO Nº 61/ 2004

PRINCÍPIOS SOBRE O TRATAMENTO DE DADOS POR VIDEOVIGILÂNCIA*

I. O problema. Enquadramento legal

1. Estão pendentes na CNPD vários pedidos de autorização de tratamentos de videovigilância. Muito embora a CNPD tenha sugerido à Assembleia da República e ao Governo⁽¹⁾ “legislação geral sobre videovigilância e outros meios electrónicos de controlo” para além da regulamentação relativa à actividade de segurança privada e aos serviços de autoprotecção, verifica-se que, até à data, não foram acolhidas as sugestões formuladas.

Para uma abordagem da utilização dos sistemas de videovigilância parece-nos adequado verificar a evolução de regimes desde que foi publicado o DL 231/98, de 22 de Julho. Este diploma permitia a adopção de *sistemas de videovigilância* no âmbito do exercício da actividade de segurança privada, os quais podiam estar a cargo de empresas privadas (art. 1.º n.º 3 al. a) ou de serviços de «autoprotecção com vista à protecção de pessoas e bens, bem como à prevenção da prática de crimes» (art. 1.º n.º 3 al. b).

Este diploma determinou a obrigatoriedade de adopção destes sistemas para o Banco de Portugal, instituições de crédito e sociedades financeiras (art. 5.º n.º 1), bem como, nomeadamente, para os estabelecimentos de restauração e bebidas que disponham de salas destinadas a dança (cf. n.º 1 da Portaria n.º 26/99, de 16 de Janeiro).

As disposições específicas de segurança para as instituições de crédito constavam do Decreto-Lei n.º 298/79, de 17 de Agosto, entretanto revogado pelo DL 35/2004, de 21 de Fevereiro..

⁽¹⁾ Pareceres n.º 22/2003, de 8 de Julho, e 41/2003, de 3 de Novembro.

Com acórdão do Tribunal Constitucional de 12 de Junho de 2002⁽²⁾, deixou de haver fundamento para a utilização de sistemas de videovigilância por parte das entidades que prestavam serviços de segurança privada, por força da declaração de inconstitucionalidade orgânica do artigo 12.º n.ºs 1 e 2 do DL 231/98

O Tribunal Constitucional – no referido acórdão – caracterizou, com rigor, as implicações deste tratamento na esfera das pessoas. Citando Paulo Mota Pinto, considerou que “a permissão da utilização dos referidos equipamentos constitui uma limitação ou uma restrição do direito à reserva da intimidade da vida privada, consignada no artigo 26.º n.º 1 da CRP”. Acrescentou que as tarefas de definição das regras e a apreciação dos aspectos relativos à videovigilância constituem «matéria atinente a direitos, liberdades e garantias».

É patente que os meios utilizados e o respectivo tratamento implicam, necessariamente, algumas restrições em relação ao direito à imagem⁽³⁾, à liberdade de movimentos, integrando esses dados, por isso, informação relativa à vida privada⁽⁴⁾.

O princípio fundamental a reter em relação à jurisprudência do Tribunal Constitucional é o de que envolvendo os sistemas de videovigilância restrições de direitos, liberdades e garantias – v.g. direito à imagem, liberdade de movimentos, direito à reserva da vida privada – caberá à lei (cf. artigo 18.º n.º 2 da CRP) decidir em que medida estes sistemas poderão ser utilizados e, especialmente, assegurar, numa situação de conflito de direitos fundamentais, que as restrições se limitem «ao necessário para salvaguardar outros direitos ou interesses fundamentais»⁽⁵⁾.

O Tribunal Constitucional tem entendido, de forma pacífica, que “nas relações entre os particulares e o Estado se introduza a noção de respeito da vida privada, de modo a que o Estado não afecte o direito ao segredo e a liberdade da vida privada, senão por via excepcional, para assegurar a protecção de outros valores que sejam superiores

⁽²⁾ Publicado na I.ª Série – A do Diário da República de 8 de Julho de 2002, pág. 5237.

⁽³⁾ Veja-se o artigo 79.º n.º 2 do Código Civil e o artigo 199.º do Código Penal.

⁽⁴⁾ Segundo J. J. Gomes Canotilho e Vital Moreira – “Constituição da República Portuguesa Anotada”, 3.ª Ed. 1993, pág. 181 – deve ser reconhecido o “direito de cada um de não ser fotografado nem ver o seu retrato exposto em público sem o seu consentimento” e o “direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar”.

⁽⁵⁾ Lucrecio Rebollo Delgado – “El Derecho Fundamental a la Intimidad”, Madrid, 2000, pág. 166 – salienta, no mesmo contexto, que “a intimidade não se refere a um sujeito concreto num espaço físico determinado. Aquela representa um direito que acompanha a pessoa independentemente do lugar onde se encontra. Desta forma, tanto a vida privada como a intimidade apresentam-se como direitos que merecem salvaguarda nos lugares públicos”.

àqueles”⁽⁶⁾. Importa, por isso, verificar que tipo de contornos são legalmente estabelecidos para assegurar o equilíbrio dos direitos fundamentais conflitantes.

2. Na sequência da referida declaração de inconstitucionalidade e da subsequente legislação entretanto publicada, nomeadamente da Lei n.º 29/2003 de 22 de Agosto, *que autorizou o Governo a legislar sobre o regime jurídico do exercício da actividade de segurança privada*, o quadro jurídico do regime da videovigilância terá que ser encontrado na aplicação das seguintes disposições legais:

- a) DL n.º 35/2004, de 21 de Fevereiro, aplicável à utilização destes meios por parte das empresas que exercem *actividade no âmbito da segurança privada*;
- b) Lei 67/98, de 26 de Outubro, na medida em que – como resulta do artigo 4.º n.º 4.º - esta lei se aplica “à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens” que permitem identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado em Portugal;
- c) O artigo 20.º do Código do Trabalho, preceito que delimitou algumas condições em que devem ser utilizados “meios de vigilância a distância no local de trabalho”.

3. É neste quadro legal que devem ser delimitadas as condições de tratamento de som e imagem, cuja captação é feita através do recurso a sistemas de videovigilância.

Um olhar pela autorização legislativa, constante da Lei 29/2003, permite evidenciar uma *preocupação fundamental* em relação às condições de utilização de equipamentos electrónicos de vigilância: deve assegurar “o *respeito pela necessária salvaguarda dos direitos e interesses constitucionalmente protegidos*” (artigo 2.º al. g). Para além disso, a Assembleia da República deixou ao Governo a tarefa de “definir, **no respeito pelo regime geral em matéria de protecção de dados**, as regras respeitantes à utilização dos equipamentos electrónicos de vigilância ..., estabelecendo que o tratamento dos dados **visa exclusivamente a protecção de pessoas e bens**, delimitando temporalmente a conservação dos dados recolhidos, garantindo o *conhecimento pelas pessoas da utilização daqueles meios*, bem como *restringindo a utilização de dados recolhidos nos termos previstos na legislação processual penal*” (artigo 2.º al. h).

⁽⁶⁾ Acórdão de 7 de Maio de 1997 (DR I.ª Série de 7/6/1997, pág. 2803) e Pierre Kayser – “La protection de la vie Privée”, 2.ª Ed., 1990, pág. 7.

Da regulamentação operada pelo DL n.º 35/2004, de 21 de Fevereiro, consideramos que merecem especial realce os seguintes aspectos:

- a) Este diploma é aplicável, **tão só**, às *entidades que exercem a actividade de segurança privada* (artigo 1.º n.º 1), enquanto «*função subsidiária e complementar da actividade das forças e dos serviços de segurança pública do Estado*» (artigo 1.º n.º 2);
- b) A actividade de segurança privada engloba duas realidades distintas. Por um lado, a “prestação de serviços a terceiros por *entidades privadas*⁽⁷⁾ com vista à protecção de pessoas e bens, **bem como à prevenção da prática de crimes**” (artigo 1.º n.º 3 al. a) e, por outro, a organização pelas entidades e em proveito próprio, para prossecução dos mesmos objectivos, de «*serviços de autoprotecção*»⁸ (al. b).
- c) É proibido, no exercício da actividade de segurança privada, “ameaçar, inibir ou restringir o exercício de direitos, liberdades e garantias ou outros direitos fundamentais” (artigo 5.º alínea b);
- d) “As entidades titulares de **alvará** ou de **licença** para o exercício dos serviços estabelecidos nas alíneas a), c) e d) do artigo 2.º, podem utilizar equipamentos electrónicos de vigilância *com o fim de protecção de pessoas e bens e ressalvados os direitos e interesses constitucionalmente protegidos*” (artigo 13.º n.º 1);
- e) “A gravação de imagens e som... devem ser conservadas pelo prazo de 30 dias, findo o qual serão destruídas, só podendo ser utilizadas nos termos da legislação penal e processual penal” (artigo 13.º n.º 2);
- f) Nos locais objecto de vigilância é obrigatória a afixação, em local bem visível, de aviso que assegure o direito de informação, nos termos do n.º 3 do artigo 13.º;
- g) “A *autorização para a utilização dos meios de vigilância electrónica nos termos do presente diploma, não prejudica a aplicação do regime geral em matéria de protecção de dados previsto na Lei 67/98, de 26 de Outubro*” (artigo 12.º n.º 4).

Para além de as empresas serem obrigadas, conforme for o caso, a possuir alvará ou licença, devem observar as exigências em relação à preservação dos direitos

⁽⁷⁾ Nos termos do artigo 22.º n.º 1 do DL n.º 35/2004, de 21 de Fevereiro, esta prestação de serviços a terceiros «só pode ser exercida com a autorização do Ministro da Administração Interna, **titulada por alvará** e após cumpridos todos os requisitos e condições estabelecidas no presente diploma e regulamentação complementar”. Sobre a emissão de alvará rege o artigo 26.º

⁽⁸⁾ Também o artigo 22.º n.º 2 DL n.º 35/2004, de 21 de Fevereiro, condiciona o exercício de actividade de «autoprotecção» a “autorização do Ministro da Administração Interna, **titulada por licença** e após cumpridos todos os requisitos e condições estabelecidas no presente diploma e regulamentação complementar” (veja-se, também, o disposto no artigo 3.º). Sobre a emissão da licença rege o artigo 27.º

liberdades e garantias das pessoas sujeitas à captação de som e imagem. A utilização de equipamentos electrónicos no âmbito das finalidades enunciadas na lei – **protecção de pessoas e bens** – obriga as entidades responsáveis a absterem-se de utilizar estes meios quando constituam ameaça, inibam ou restrinjam o exercício de direitos, liberdades e garantias ou outros direitos e interesses constitucionalmente protegidos.

4. Esta preocupação do legislador é claramente consentânea, no nosso ponto de vista, com os pressupostos estabelecidos pela Lei 67/98, de 26 de Outubro. Até à publicação de legislação geral de enquadramento sobre a utilização de sistemas de videovigilância, consideramos que a Lei 67/98 surge como legislação geral a que deve obedecer o tratamento operado por sistemas de videovigilância e de outras formas de captação, difusão de sons e imagens. É o próprio DL 35/2004 que, no seu artigo 13.º n.º 4, aponta para a aplicação subsidiária da Lei 67/98, designadamente em sede de «direito de acesso à informação, oposição aos tratamentos e regime sancionatório».

Por força da aplicação da Lei 67/98, os responsáveis pelo tratamento de imagem e som estão obrigados, em particular, a notificar estes tratamentos à CNPD (art. 27.º n.º 1), a observar os princípios relativos à qualidade dos dados (artigo 5.º), a respeitar as “condições de legitimidade” e de licitude para poderem tratar esses dados (artigos 6.º, 7.º e 8.º) e a assegurar o direito de informação (art. 10.º). Os dados devem ser conservados por prazos limitados, cabendo à CNPD fixar o prazo de conservação em função da finalidade (artigo 23.º n.1 al. f). Não nos parece, igualmente, que possa ser afastado o direito de oposição quando se verificarem os requisitos do artigo 12.º al. a).

Mas, em função da natureza dos dados e da forma como são recolhidos, interessa saber se as entidades têm legitimidade para proceder ao seu tratamento, continuando a realizar a captação de som e imagem.

Por força do artigo 35.º n.º 3 da CRP – e porque estamos perante dados da «vida privada» (cf. a doutrina do Tribunal Constitucional) – o tratamento só pode ser realizado quando houver «autorização prevista em lei» ou «consentimento dos titulares»⁽⁹⁾. A CNPD deve, no caso concreto, apurar se será admissível o tratamento à luz do artigo 35.º n.º 3 da CRP e do artigo 7.º n.º 2 e 3 da Lei 67/98.

Isto é, para além dos casos em que a lei admite a possibilidade de utilização de sistemas de videovigilância no âmbito de certas actividades específicas (o caso do

⁽⁹⁾ Admitimos que, em face dos perigos que envolve para a privacidade e intimidade da vida privada dos habitantes de um imóvel (v.g. condomínio fechado), a única condição que pode legitimar a colocação de sistemas de videovigilância será o consentimento das pessoas aí residentes (condóminos e arrendatários).

referido DL n.º 35/2004, de 21 de Fevereiro), há situações em que *é a própria lei* que impõe ou admite a utilização de sistemas de videovigilância:

- a) A Lei 38/98, de 4 de Agosto, obrigou os organizadores de competições desportivas a dotarem os seus recintos de sistemas de videovigilância;
- b) O DL 139/2002, de 17 de Maio, obriga os estabelecimentos de fabrico e armazenagem de produtos explosivos a “estarem protegidos por um sistema de vigilância permanente que assegure a detecção de intrusos”, admitindo que uma das opções de controlo possa passar pela adopção de um “sistema de videovigilância instalado nos termos da lei geral” (artigo 22.º n.º 2 e 3 alínea b);
- c) Outras disposições admitem a sua utilização quando esta se justifique em função de determinado tipo de actividades (cf. artigo 20.º n.º 2 do Código do Trabalho). Também se deve admitir, no mesmo contexto, a utilização destes sistemas para controlo de postos de trabalho que apresentem especiais riscos para os trabalhadores, quer pela sua especial perigosidade em relação ao manuseamento de certas substâncias perigosas, quer pela inacessibilidade ou especial solidão em que os trabalhadores exercem a sua actividade (vg. minas, centrais nucleares, laboratórios em que sejam manuseados produtos químicos perigosos).

Mas, para além da admissibilidade legal de sistemas de videovigilância, importa verificar que outros «fundamentos de legitimidade» podem servir de base à autorização da CNPD.

Perante a previsão do artigo 7.º n.º 2 e 3 da Lei 67/98 é admissível que, *em abstracto*, possa haver situações em que a utilização de sistemas de videovigilância pode estar fundamentada na defesa de «interesses vitais dos titulares» (n.º 3 al. a) ou para «declaração, exercício ou defesa de um direito em processo judicial» (n.º 3 al. d).

Importa saber, igualmente, se a utilização de sistemas de videovigilância pode ser fundamentada na necessidade de assegurar a prevenção de crimes ou na “documentação” da prática de infracções penais – nomeadamente no contexto da finalidade de «protecção de pessoas e bens». O tratamento só será, no entanto, legítimo se se apresentar como necessário à execução de finalidades legítimas do seu responsável e desde que “não prevaleçam os direitos, liberdades e garantias do titular dos dados” (artigo 8.º n.º 2 da Lei 67/98). É ainda necessário, como resulta do preceito acabado de citar, que este tratamento seja autorizado pela CNPD, que

verificará se foram observadas as normas de protecção de dados e de segurança da informação.

A tarefa de enquadramento jurídico em relação às «condições de legitimidade» foi objecto de profundo debate no seio da CNPD, não havendo consenso sobre esta temática.

II. A abordagem da videovigilância por parte de outras autoridades e a experiência noutros países

1. Um olhar pela doutrina e experiência noutros países, especialmente ao nível de autoridades de protecção de dados, permite confirmar que as linhas delineadas pelo Tribunal Constitucional, baseadas no princípio da proporcionalidade, dominam, de forma decisiva, as condições de tratamento de dados que recorram a sistemas de videovigilância.

O *Conselho da Europa* estabeleceu alguns princípios a adoptar em relação ao tratamento de som e imagem em matéria de videovigilância⁽¹⁰⁾. Um dos aspectos relevantes que o documento sublinhou refere-se à ponderação, em termos de proporcionalidade, entre as exigências de segurança e a protecção da vida privada. Adianta, ainda, que “os sistemas de videovigilância podem produzir efeitos positivos em termos de segurança. A eficácia dos seus efeitos não é uniforme. Algumas aplicações traduziram-se numa diminuição de actos ilícitos em espaços públicos. Outras mostraram-se ineficazes ou afastaram a criminalidade para zonas limítrofes ou limitaram-se a oferecer meios de prova em relação às pessoas observadas”⁽¹¹⁾.

Na apreciação dos efeitos decorrentes da introdução dos sistemas de videovigilância não podem deixar de ser analisados os “efeitos potenciais sobre a liberdade e comportamento dos cidadãos”, fazendo-se uma necessária reflexão “sobre o grau de violação da vida privada” que tenha especial incidência nas vertentes da «liberdade de circulação» e na análise de «comportamentos».

Em matéria de pertinência é fundamental que os responsáveis pela recolha de imagens:

⁽¹⁰⁾ <http://www.legal.coe.int>

⁽¹¹⁾ Lucrecio Rebollo Delgado (“El Derecho Fundamental a la Intimidad”, Madrid, 2000, pág. 168) considera, em sentido similar, que “a videovigilância não opera como elemento dissuasor da prática de delitos; representa, na sua essência, um elemento de prova da realização dos mesmos”.

- a) Definam a localização das *cameras* e as modalidades de registo (registo e conservação das imagens, ângulos utilizados, escolha de «grandes planos» e *scanner* de imagens);
- b) Reduzam o campo visual em função da finalidade prosseguida ou das zonas em que “a videovigilância é efectivamente necessária, dando uma atenção particular aos casos em que as *cameras* – filmando lugares públicos – permitem o registo de som e imagem em lugares privados situados na proximidade”;
- c) Procedam à recolha de imagens no estritamente necessário à finalidade prosseguida, sendo dispensáveis grandes planos ou detalhes não relevantes em função dos objectivos a que se propõe o responsável.

O *Grupo do Artigo 29.º* – Grupo de Protecção de Dados Pessoais – aprovou, em 11 de Fevereiro de 2004, o Parecer n.º 4/2004 sobre o tratamento de dados pessoais por meio de videovigilância⁽¹²⁾. Nesse documento foi salientada a necessidade de as entidades evitarem a «utilização desproporcionada» da videovigilância. O princípio da proporcionalidade exige uma apreciação sobre a «qualidade dos dados» (adequação, pertinência e carácter não excessivo – cf. artigo 6.º da Directiva n.º 95/46/CE de 24 de Outubro de 1995) e avaliação de alguns aspectos sobre a forma como é feito o tratamento.

As considerações feitas por este Grupo em relação à «legitimidade do tratamento» merecem particular realce, nomeadamente quando salientam a necessidade de assegurar que a vigilância esteja «em conformidade com as disposições gerais e específicas aplicáveis a esse sector». Admitindo-se que a legislação privilegia os fins de «segurança pública», importa considerar os princípios aplicáveis em matéria de «direito à imagem» ou à protecção do domicílio e dar particular realce ao facto de, em geral, as imagens serem recolhidas em lugares públicos ou de acesso ao público.

Esta autoridade salienta que «se o equipamento tiver sido instalado por entidades privadas ou por organismos públicos, especialmente por órgãos da administração local, alegadamente por *motivos de segurança ou para detecção, prevenção e controlo da criminalidade*, deverá ter-se especial cautela na **determinação e informação desses fins**, quanto às tarefas que poderão ser legalmente desempenhadas pelo responsável pelo tratamento».

⁽¹²⁾ Disponível in http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Haverá casos em que a realização de um tratamento passa pela obtenção do consentimento. Se assim for, o consentimento «terá de ser dado separada e especificamente para actividades de vigilância que envolvam locais onde decorre a vida privada de uma pessoa». Será de avaliar, ainda, a hipótese de tratamento de dados relativos a infracções (n.º 5 do artigo 8.º da Directiva).

2. Os Estados tendem a colocar o acento tónico da utilização da videovigilância em razões específicas e em preocupações muito próprias. Por exemplo, em Espanha há uma preocupação especial na regulação da utilização de *cameras* pelas forças policiais. Segundo Ricard Martinez⁽¹³⁾ «em Espanha o emprego das *cameras* de vídeo surge com fundamento na prevenção das acções realizadas por membros de organizações independentistas no País Basco e enquadra-se no âmbito de uma política anti-terrorista. Por seu turno, os casos francês e italiano parecem responder melhor à luta contra a delinquência comum». No caso português anota-se, de forma marcante, o objectivo de assegurar a «protecção de pessoas e bens».

3. A *Autoridade de controlo grega* – numa decisão de 26 de Setembro de 2000⁽¹⁴⁾ – estabeleceu Directivas sobre a recolha de som e imagem através de circuitos fechados de televisão (CCTV). Começou por fixar, no artigo 1.º, os critérios a considerar em termos de legitimidade do tratamento de dados:

A – O *princípio da necessidade* – O tratamento é permitido quando a finalidade não puder ser alcançada por qualquer outro meio igualmente eficaz, mas menos intrusivo para o cidadão;

Princípio da proporcionalidade – O interesse legítimo do responsável deve prevalecer sobre os direitos e interesses do indivíduo a que dizem respeito, desde que os seus direitos fundamentais não sejam violados.

B – Os dados recolhidos por CCTV devem ser adequados, pertinentes e não excessivos em relação à finalidade para a qual são usados. Portanto, os locais onde as *cameras* fixas de vídeo devem ser instaladas, bem como a forma de gravação, deve ser de maneira a que não seja gravada mais informação da que for necessária para a finalidade.

C – Em espaços abertos as *cameras* de vídeo devem ser instaladas em locais que não lhes permitam captar imagens em entrada ou interior de residências privadas.

⁽¹³⁾“El Control por el Garante italiano para la Protección de los Datos Personales de los Ficheros y Archivos de Imágenes Policiales” in <http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=15> pág. 1.

⁽¹⁴⁾ <http://www.dpa.gr>

A *autoridade de controlo belga* – no seu parecer 34/1999, de 13 de Dezembro, relativo ao tratamento de imagens efectuadas por sistemas de videovigilância⁽¹⁵⁾ – chamou particular atenção para o princípio da proporcionalidade, dando especial realce à necessidade de o “interesse geral ou interesses legítimos do gestor do tratamento serem balanceados com o direito à protecção da vida privada da pessoa objecto de registo”.

No balanceamento entre o princípio da proporcionalidade e os riscos para a vida privada das pessoas, o campo coberto pelas *cameras* deverá limitar as possibilidades de identificação das pessoas visadas.

Em relação à colocação de *cameras* em locais públicos deve atender-se aos efeitos causados em relação à captação de lugares não acessíveis ao público e considerar que as imagens se devem apresentar como um meio adequado e necessário à realização do objectivo prosseguido.

A *autoridade de protecção de dados italiana – Garante per la Protezione dei Dati Personali* – teve oportunidade de considerar, numa decisão de 2 de Dezembro de 1998, que os aspectos relativos à «pertinência» (cf. artigo 9.º da Lei 675/1996) são fundamentais. Por isso, entendeu que «o material informático que se pode adquirir no âmbito de uma investigação penal deve estar ligado com as necessidades e finalidades de prevenção, de investigação e de repressão do delito».

Numa nota de imprensa, de 10 de Fevereiro de 1999, o Garante salientou, na sequência de reunião havida com altos responsáveis policiais, que era fundamental manter uma certa vigilância sobre a aplicação das normas no domínio da prevenção e investigação, tendo sempre presente que “*é preciso ponderar as finalidades de prevenção e repressão dos delitos com o respeito pela dignidade das pessoas*”⁽¹⁶⁾.

4. Como referimos, a *legislação espanhola* teve uma preocupação especial em regular a utilização de *cameras* por Forças e Corpos de Segurança em lugares públicos. A Ley Orgánica 4/1997, de 4 de Agosto, e a respectiva regulamentação operada pelo Real Decreto 596/1999, de 16 de Abril, fixaram as condições de instalação e utilização de *cameras*. Conforme resulta do preâmbulo do Real Decreto 596/1999, pretendeu-se «colocar à disposição das Forças e Corpos de Segurança o emprego de meios para *prevenção de delitos, a protecção de pessoas e a custódia de bens em espaços*

⁽¹⁵⁾ <http://www.privacy.fgov.be>

⁽¹⁶⁾ Veja-se Ricard Martinez – “El Control por el Garante italiano para la Protección de los Datos Personales de los Ficheros y Archivos de Imágenes Policiales” in <http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=15> pág. 7.

públicos, sendo que a sua finalidade primordial consiste em estabelecer as garantias necessárias para que a referida utilização seja estritamente respeitadora dos direitos e liberdades dos cidadãos».

A colocação destes dispositivos está sujeita a uma autorização administrativa prévia. A lei prevê, de forma expressa, a colocação das imagens à disposição das autoridades judiciais quando as gravações captem factos que possam ser qualificados como ilícitos penais. Em geral, as imagens são destruídas a fim de um mês.

O direito de informação deve ser assegurado, através de uma placa informativa na qual figurará um pictograma de uma *camera* de vídeo e uma descrição genérica da zona de vigilância e das autoridades responsáveis pela autorização e guarda das gravações.

O Conselho Permanente do Conselho de Estado espanhol – no Parecer n.º 549/1999, de 25 de Março⁽¹⁷⁾ – salientou a necessidade de preservar a intimidade das pessoas “que pode ser violada com a utilização de novas tecnologias audiovisuais”, lembrando que deve ser compatibilizada com a obrigação que os poderes públicos têm de velar pela segurança das próprias pessoas. Daí a «necessidade de ponderação de acordo com o que, numa sociedade democrática, constituem medidas necessárias...para a segurança nacional, a segurança pública, a defesa da ordem e a prevenção de delitos».

A jurisprudência espanhola tem entendido, em geral, que a recolha de imagens só poderá ser feita sem autorização judicial quando realizada “em espaços, lugares ou locais livres e públicos, em estabelecimentos oficiais, bancários ou empresariais”⁽¹⁸⁾.

Em *França*, a Lei n.º 95-73, de 21 de Janeiro de 1995, estabeleceu o quadro relativo à orientação e programação relativa à segurança. No seu artigo 10.º prevê a possibilidade de utilização de sistemas de videovigilância “na via pública para protecção das instalações úteis à defesa nacional, a regulação do tráfego...a prevenção e segurança de pessoas e bens nos locais particularmente expostos a riscos de agressão e de roubo”. A utilização destes meios é ainda possível nos “lugares e estabelecimentos abertos ao público particularmente expostos a riscos de agressão ou de roubo, a fim de velar pela segurança das pessoas e bens”⁽¹⁹⁾.

⁽¹⁷⁾ In <http://www.uc3m.es/uc3m/dpto/PU/dppu02/dce549-1999.htm>

⁽¹⁸⁾ Entre muitos, vejam-se as Sentenças do Tribunal Supremo n.º 353/1996, de 19 de Abril (Rec. 779/1995) e n.º 620/1997, de 5 de Maio (Rec. 1868/1994).

⁽¹⁹⁾ Para um melhor enquadramento constitucional veja-se a Decisão do Conselho Constitucional n.º 94-352 DC de 18 de Janeiro de 1995 (in <http://www.conseil-constitutionnel.fr>). Nesta decisão reconheceu o Conselho Constitucional que estão em causa vários direitos fundamentais constitucionalmente protegidos:

A utilização destes meios está condicionada à “informação do público, de maneira clara e permanente, sobre a existência do sistema de videovigilância e sobre a autoridade ou pessoa responsável”. A instalação dos equipamentos está dependente de autorização da prefeitura («*préfecture*») do lugar da instalação ou, em Paris, pela “prefeitura de polícia” («*préfecture de police*»)²⁰. Existe uma «Comissão Departamental dos Sistemas de Videovigilância» que integra 5 membros.

A prefeitura põe à disposição do público a lista das autorizações, indicando a data da autorização e o serviço ou a pessoa responsável (artigo 16.º do Dec. 96-926).

III. A apreciação das condições de legitimidade

1. Como já referimos, é possível, em abstracto, fundamentar e legitimar o tratamento numa disposição legal ou no consentimento (cf. artigo 7.º n.º 2 da Lei 67/98), na protecção de interesses vitais²¹ (art. 7.º n.º 3 al. a) ou no exercício e defesa de um direito em processo judicial (art. 7.º n.º 3 al. d).

Porém, importa não perder de vista que a esmagadora maioria dos pedidos de notificação tem como finalidade assegurar a «**protecção de pessoas e bens**», tendo como pano de fundo a utilização das imagens como prova das infracções criminais praticadas, em observância das disposições processuais penais.

Ora, estando em causa objectivos relacionados com a prevenção de crimes, entendemos que o fundamento de legitimidade poderá, nestes casos, ser encontrado na previsão do artigo 8.º n.º 2 da Lei 67/98, de 26 de Outubro. A autorização da CNPD (cf. artigo 28.º n.º 1 al. a) terá que respeitar os diversos pressupostos estabelecidos naquele preceito.

Muito embora o artigo 8.º n.º 2 se refira ao tratamento relativo a «*suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias*», não podemos deixar de considerar que a redacção abrangente do preceito (suspeitas de actividades ilícitas e infracções penais), a própria sistematização da Lei 67/98 e a realidade quotidiana – nomeadamente no âmbito das actividades policiais, também vocacionadas para a prevenção criminal – só podem levar-nos a concluir no sentido de que as tarefas de

“a liberdade individual que deve ser assegurada pela autoridade judiciária” (cf. art. 66.º da Constituição), a “liberdade de movimentos sem controlo arbitrário e generalizado e o direito ao respeito da vida privada que implica o direito ao anonimato”.

⁽²⁰⁾ Veja-se o artigo 1.º do Décret n.º 96-926 de 17 de Outubro de 1996.

⁽²¹⁾ Um exemplo do recurso a sistemas de videovigilância em ambiente hospitalar será o controlo e monitorização de doentes (v.g. cuidados intensivos).

recolha e tratamento de informação no contexto da *prevenção criminal* se devem enquadrar neste preceito⁽²²⁾.

Sendo pressuposto que as imagens recolhidas possam servir de prova em processo penal (cf. o artigo 13.º n.º 2 do DL 35/2004) não podemos deixar de considerar esta finalidade e englobar a recolha de dados, bem como a obtenção dos meios de prova, numa estratégia integrada que visa a protecção de pessoas e bens. Ou seja, para além de estar em causa, objectivamente, a *prevenção e dissuasão da prática de actos ilícitos* – tarefa que é desempenhada na prossecução do interesse público, em complementaridade e subsidiariedade face às competências das forças e serviços de segurança – a informação recolhida pode vir a ser utilizada como prova da infracção. Daí que não seja para nós curial autonomizar, de forma estanque, o processo de tratamento de videovigilância do contexto mais amplo das finalidades de prevenção criminal, da existência de suspeitas ou da verificação de infracções penais.

Conforme refere o Tribunal Constitucional⁽²³⁾, “as funções de recolha e tratamento de informações, as de actividade de vigilância e fiscalização a levar a cabo pelas várias entidades competentes nessa área, **exactamente porque preventivas e dissuasoras**, estão direccionadas para a generalidade das pessoas e dos locais sobre que incidem ou são de matriz específica desmotivadora, mas não se orientam para uma actividade investigatória de crimes praticados”.

Por isso, não será legítimo defender que todas as pessoas que frequentam os locais públicos sujeitos a videovigilância se apresentam como «potenciais suspeitos». O que está em causa na utilização destes meios é assegurar a dissuasão, **sempre com o conhecimento das pessoas e com protecção dos seus direitos fundamentais**⁽²⁴⁾, bem como registar e documentar a eventual prática de infracções. O tratamento de som ou imagem e a finalidade delineada pelo responsável, porque assume objectivos primordialmente preventivos e dissuasores, não tem que “situar-se, necessariamente,

⁽²²⁾ Deve anotar-se que o artigo 11.º n.º 2 da Lei 67/98, que estabelece condicionantes em relação ao direito de acesso, limita o exercício do direito de acesso quando estão em causa finalidades relativas à «*prevenção ou investigação criminal*».

⁽²³⁾ Acórdão n.º 456/93, de 12 de Agosto de 1993 in DR I.ª Série A de 9 de Setembro de 1993, pág. 4815.

⁽²⁴⁾ O artigo 8.º n.º 2 obriga, como condição a ponderar pela CNPD, a que «não prevaleçam os direitos, liberdades e garantias dos titulares dos dados». Em geral, o êxito das diligências de observação e vigilância está dependente da ignorância por parte do visado do facto de que está a ser objecto de escutas, de gravação de som e imagem. A doutrina do Tribunal Europeu dos Direitos do Homem, relativa às escutas telefónicas e à possível violação do artigo 8.º da CEHD, salientou que “a natureza secreta desta modalidade de diligência apresenta riscos de abusos e, por conseguinte, a intervenção realizada só pode considerar-se «necessária numa sociedade democrática» se o sistema de vigilância se rodear de garantias suficientes” (Caso Malone de 2 de Agosto de 1984). Para maior desenvolvimento veja-se José Francisco Etxeberria Guridi – “La Protection de los Datos de Carácter Personal en el Ámbito de la Investigación Penal”, 1998, pág. 291.

a montante de qualquer actividade delituosa”⁽²⁵⁾ ou pressupor a existência de suspeitas concretas sobre a generalidade das pessoas em relação às quais são captadas as imagens.

Como se salienta no Parecer da Procuradoria-Geral da República n.º 95/2003, de 6 de Novembro⁽²⁶⁾ em relação à prevenção criminal levada a cabo pela polícia – com referência ao acórdão do Tribunal Constitucional n.º 456/93 (citado) – os «actos de polícia de natureza preventiva» podem decorrer da vigilância ou ser independentes dela: «umas vezes configuram-se como actos genéricos, dirigindo-se a uma pluralidade de pessoas; outras vezes como actos individuais. A vigilância genérica poderá ser essencialmente preventiva; por seu lado, a vigilância individualmente dirigida apresentar-se-á, na normalidade dos casos, mais como acto de averiguação ou, então, de prevenção directa determinada pela prévia existência de elementos de suspeita relativamente a algum comportamento individual».

Estes conceitos e princípios são aplicáveis à realidade da videovigilância levada a efeito pelas entidades responsáveis que decidem avançar com o tratamento vocacionado para a «protecção de pessoas e bens». A recolha de som e imagem não está direccionada, em geral, para actos individuais mas abrange o universo das pessoas – não se sabe quais – que frequentam o estabelecimento e sem que haja, à partida, a mínima suspeição sobre a sua conduta. As imagens só têm relevância e só são «pertinentes» (cf. artigo 5.º n.º 1 al. c) da Lei 67/98) quando ocorrer algum facto com relevância em sede de investigação criminal. Neste caso serão as imagens encaminhadas para a autoridade competente.

O som e as imagens – recolhidas para poderem ser utilizadas nos termos da lei penal – representam um tratamento que não tem em vista «vigiar suspeitos» mas, porque essencialmente fundamentado em objectivos de prevenção e dissuasão de futuros factos criminosos, servir de meio de prova em caso de prática de actividades delituosas.

Importa reconhecer, como alguém já referiu, que “fora da esfera íntima da sua vida privada, a pessoa física encontra-se permanentemente exposta ao exame do público”⁽²⁷⁾, nomeadamente se as suas condutas ocorrem em locais públicos. É fundamental salientar, por outro lado, que o facto de as imagens serem recolhidas em lugares públicos e os titulares dos dados serem previamente informados da existência

⁽²⁵⁾ Veja-se, em relação à actuação policial, Marcello Caetano – “Manual de Direito Administrativo”, Coimbra, 9.ª Edição, II Vol. pág. 1145.

⁽²⁶⁾ In DR II.ª Série de 4 de Março de 2004, pág. 3706.

⁽²⁷⁾ Parecer da PGR n.º 95/2003, de 6 de Novembro de 2003 (in DR II.ª Série de 4 de Março de 2004, pág. 3703).

de tratamento e das suas finalidades contribui, substancialmente, para afastar a ideia de que existe uma captação ou utilização arbitrária da sua imagem. Aliás, na linha do que dispõe o artigo 13.º n.º 2 do DL 35/2004, as imagens só podem ser utilizadas nos termos da lei processual penal.

Em face do exposto a CNPD propõe-se autorizar o tratamento de som e imagem quando, observados os princípios relativos à qualidade dos dados (artigo 5.º), o direito de informação (artigo 10.º), as «condições de legitimidade» (artigo 7.º e 8.º n.º 2) e demais princípios da Lei 67/98 que, no caso concreto, forem exigíveis.

2. De entre as condições a observar importa conferir particular atenção – quando aplicável o artigo 8.º n.º 2 da Lei 67/98 – aos pressupostos em que assenta o tratamento e se é determinado pela necessidade de «execução de finalidades legítimas do seu responsável». Para além disso, é exigível que, por força desse tratamento, «não prevaleçam os direitos, liberdades e garantias do titular dos dados. Porque estão em conflito direitos passíveis de protecção – o direito de propriedade, à segurança de pessoas e bens, de um lado, e o direito à intimidade, de outro – este preceito condiciona o tratamento à necessidade de ponderação entre o interesse e finalidades legítimas dos responsáveis e os direitos, liberdades e garantias dos titulares dos dados que podem ser afectados pela recolha de imagens.

O tratamento a realizar e os meios utilizados devem ser considerados os **necessários, adequados e proporcionados** com as finalidades estabelecidas: a protecção de pessoas e bens. Ou seja, para se poder verificar se uma medida restritiva de um direito fundamental supera o juízo de proporcionalidade importa verificar se foram cumpridas três condições: se a medida adoptada é idónea para conseguir o objectivo proposto (*princípio da idoneidade*); se é necessária, no sentido de que não exista outra medida capaz de assegurar o objectivo com igual grau de eficácia (*princípio da necessidade*); se a medida adoptada foi ponderada e é equilibrada ao ponto de, através dela, serem atingidos substanciais e superiores benefícios ou vantagens para o interesse geral quando confrontados com outros bens ou valores em conflito (*juízo de proporcionalidade em sentido restrito*)²⁸.

Na linha do que referimos, será admissível aceitar que – quando haja razões justificativas da utilização destes meios – a gravação de imagens se apresente, em

⁽²⁸⁾ Veja-se, para maior desenvolvimento e no mesmo sentido, o Parecer da PGR n.º 95/2003, loc. cit. pág. 3705.

primeiro lugar, como medida preventiva ou dissuasora tendente à protecção de pessoas e bens e, ao mesmo tempo, como meio idóneo para captar a prática de factos passíveis de serem considerados .

como ilícitos penais e, nos termos da lei processual penal, servir de meio de prova.

Estamos perante a aplicação do princípio da proporcionalidade que “implica, em cada caso concreto, a idoneidade do meio utilizado – a videovigilância – bem como, e também, o respeito pelo princípio da intervenção mínima”.

O princípio da intervenção mínima obriga, necessariamente, que, em cada caso concreto, se pondere entre a finalidade pretendida e a necessária violação de direitos fundamentais, aqui concretamente o direito à privacidade e à imagem.

Deverá mesmo pressupor-se que, no caso concreto, o risco a prevenir deverá ser de todo razoável⁽²⁹⁾ e proporcionado quando comparado com os direitos fundamentais de terceiros que são afectados com a utilização destes meios.

Como ensina Vieira de Andrade⁽³⁰⁾, “não pode ignorar-se que nos casos de conflito, a Constituição protege diversos valores ou bens em jogo e que não será lícito sacrificar pura e simplesmente um deles ao outro”. Adianta este autor que “a medida em que se vai comprimir cada um dos direitos (ou valores) pode ser diferente, dependendo do modo como se apresentam e das alternativas possíveis de solução de conflito”.

Por isso, em cada caso concreto e de acordo com os princípios acabados de enunciar, a CNPD deverá limitar ou condicionar a utilização de sistemas de videovigilância quando a utilização destes meios se apresentem como excessivos e desproporcionados aos fins pretendidos e tenham consequências gravosas para os cidadãos visados.

IV. O acesso aos dados recolhidos pelos sistemas de videovigilância

1. Sendo patente que os sistemas de videovigilância estão direccionados para o desempenho de finalidades relativas à «protecção de pessoas e bens», apresentando-se como medida preventiva e de dissuasão em relação à prática de infracções penais e podendo, ao mesmo tempo, servir de prova nos termos da lei processual penal, é

⁽²⁹⁾ Veja-se a Deliberação n.º 98/2002, de 21 de Maio.

⁽³⁰⁾ “Os Direitos Fundamentais na Constituição de 1976, 1983, pág. 221

imprescindível que – de acordo com o *princípio da necessidade* – o acesso às imagens seja restrito às entidades que delas precisam para alcançar as finalidades delineadas. Uma vez detectada a prática de infracção penal, a entidade responsável pelo tratamento deve – com a respectiva participação – enviar ao órgão de polícia criminal ou à autoridade judiciária competente as imagens recolhidas. Não há qualquer justificação para a visualização das imagens por parte das entidades responsáveis por duas ordens de fundamentos:

- a) Caso não tenha sido praticada qualquer infracção penal ou procedimento que atente contra as pessoas e bens, a visualização de imagens não tem qualquer sentido útil, sob pena de violação do disposto no artigo 5.º n.º 1 alínea b) da Lei 67/98, de 26 de Outubro;
- b) Caso tenha sido praticada infracção penal as imagens devem, necessariamente, ser canalizadas para a autoridade competente.

A CNPD considera que os produtores destes sistemas devem por em prática medidas de segurança adequadas para impedir a difusão ou acesso não autorizado, por forma a garantir que os responsáveis dos tratamentos cumpram as medidas de segurança a que estão vinculados por força dos artigos 14.º e 15.º da Lei 67/98, de 26 de Outubro. Perante esta realidade tanto o Grupo do Artigo 29.º como a autoridade italiana de protecção de dados também já sugeriram a adopção de uma solução “que consiste no *uso de duas chaves de acesso* – podendo uma delas estar na posse do responsável pelo tratamento e outra na da polícia – metodologia que será útil para garantir que as imagens são visualizadas apenas pelo pessoal da polícia e não por pessoal não autorizado”⁽³¹⁾.

2. Admite-se, excepcionalmente, a visualização das imagens quando – *não havendo qualquer infracção penal* – os titulares dos dados tenham solicitado o «direito de acesso», nos termos do artigo 11.º da Lei 67/98. O responsável do tratamento não está dispensado de assegurar o direito de acesso⁽³²⁾, razão pela qual lhe é exigível que procure a imagem captada em relação à pessoa visada que exerceu aquele direito.

⁽³¹⁾ Locais citados.

⁽³²⁾ No direito francês o artigo 10.º da Lei 95-73, de 21 de Janeiro, estabelece que qualquer interessado pode dirigir-se ao responsável do tratamento de videovigilância para obter um acesso aos registos que lhe dizem respeito ou de verificar a sua destruição no prazo previsto. Também o Decreto n.º 96-926, de 17 de Outubro, estabelece que o pedido de autorização prévia à instalação de um sistema de videovigilância deve especificar as modalidades do direito de acesso por parte do interessado (artigo 1.º n.º 10).

No entanto, e porque o exercício do direito de acesso por parte de determinado interessado pode envolver o acesso a dados de terceiros, o responsável do tratamento deve tomar todas as medidas técnicas necessárias para ocultar/anonimizar as imagens de terceiros.

Quando estiverem em causa imagens que servem de prova em processo criminal – imagens necessariamente sujeitas às regras do segredo de justiça – é aplicável o disposto no artigo 11.º n.º 2 da Lei 67/98 (prevenção ou investigação criminal), razão pela qual os pedidos de acesso devem ser encaminhados para a CNPD⁽³³⁾.

3. Será admissível, igualmente, que determinadas pessoas – que não sejam os responsáveis pelos tratamentos – possam solicitar, no âmbito de processo criminal, o acesso às imagens para assegurar o «exercício ou defesa de um direito em processo judicial» e exclusivamente para essa finalidade (cf. artigo 7.º n.º 3 alínea d) da Lei 67/98). Isto é, determinado cidadão ou entidade que tenha sido lesado por determinada actuação ou procedimento captado por sistemas de videovigilância não estará inibido, com base no preceito citado, de poder beneficiar da prova captada para exercício dos seus direitos no contexto de participação criminal. Neste caso as imagens serão enviadas à autoridade judiciária ou órgão de polícia criminal competente.

Lisboa, 19 de Abril de 2004

Amadeu Guerra (relator), Alexandre Pinheiro, Luís Durão Barroso, Eduardo Campos,
Ana Luísa Geraldes, Luís Lingnau da Silveira (Presidente)

⁽³³⁾ Solução idêntica foi adoptada no direito francês, que admite a recusa do direito de acesso quando fundamentada em razões de segurança do Estado, da defesa e segurança pública ou de direitos de terceiros (artigo 10.º V da Lei 95-73, de 21 de Janeiro).