“1. A todos são reconhecidos os direitos (...) à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.
2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias”

Constituição da República Portuguesa (artigo 26º)

“A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.”

Constituição da República Portuguesa (artigo 18º)

Contributo da Associação D3 – Defesa dos Direitos Digitais
para os trabalhos da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, da Assembleia da República, a propósito da Proposta de Lei 111/XIV/2 - *Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança*

O presente documento pode ser publicado na íntegra.

16 de Novembro de 2021

No passado dia 6 de Setembro de 2021 deu o Governo entrada na Assembleia da República da Proposta de Lei 111/XIV/2, que visa regular utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança, revogando a lei actualmente em vigor - Lei n.º 1/2005, de 10 de janeiro.

O presente parecer constitui um contributo da Associação D3 – Defesa dos Direitos Digitais, para os trabalhos da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, da Assembleia da República.

Introdução

Existe uma ligação directa entre a Democracia e a Segurança. A um Estado, é sempre possível implementar mais e mais eficientes medidas de Segurança, sejam elas tecnológicas ou não. No entanto, somente Estados totalitários almejam alcançar, pela supressão de direitos, uma segurança ilimitada. Pelo contrário, Estados democráticos entendem o conceito de segurança enquanto uma segurança necessariamente relativa, que tem como limite inegociável os direitos, liberdades e garantias dos cidadãos.

Com a evolução tecnológica, torna-se possível e tentador vigiar de forma cada vez mais intensa e eficiente, aumentando assim o controlo sobre os cidadãos, por forma a tentar limitar os crimes ou ataques à segurança do Estado. Sob tal desígnio, nos últimos anos, Estados totalitários têm tornado realidade distopias tecnológicas até agora só imaginadas em obras de ficção científica. Em contra-corrente, a Europa, ao mesmo tempo que também desenvolve o seu sector tecnológico, tem reforçado os seus princípios de defesa dos direitos fundamentais dos cidadãos europeus, em especial a defesa do direito à privacidade e do direito à protecção de dados. Não que não tenha à sua disposição exactamente as mesmas tecnologias, simplesmente compreende-se que não é por ser tecnologicamente possível vigiar melhor que se deve necessariamente fazê-lo. Bem pelo contrário: uma Democracia que tenha por objectivo o alcançar de uma segurança absoluta, rapidamente deixa de o ser.

Há então que saber traçar os limites.

No nosso regime constitucional, a restrição de direitos fundamentais dos cidadãos apenas é possível quando tal restrição respeite o princípio da proporcionalidade. Como resulta do art. 18º/2 da Constituição da República Portuguesa e de consensual jurisprudência constitucional, a restrição de direitos fundamentais só é admissível se tal restrição for demonstradamente:

- **adequada** ao fim visado (a medida tem de ser apropriada a alcançar o fim que se visa alcançar)
- **necessária** (ser indispensável, no sentido de não existir uma alternativa eficaz que seja menos lesiva aos direitos fundamentais dos cidadãos)
- **proporcional** em sentido estrito (proibição do excesso; não ir além do estritamente necessário).

O teste da proporcionalidade tem como requisitos a verificação cumulativa de cada um destes três sub-princípios do princípio da proporcionalidade. O incumprimento de qualquer deles torna a medida necessariamente inconstitucional.

Infelizmente, e como veremos, a Proposta de Lei 111/XIV/2 não viola apenas o princípio da proporcionalidade como revela um desprezo absoluto pelo regime constitucional de restrição de direitos fundamentais: não cumpre, e nem sequer tenta cumprir.

Sumário

Tal como configurada, a presente proposta cria a base legal para a banalização da videovigilância em Portugal, agravada pela utilização desregrada de mecanismos de inteligência artificial e de drones por parte de autoridades policiais.

Entre outras coisas, a presente proposta de lei:

- Retira o carácter excepcional à utilização de videovigilância, alargando os fins que justificam a sua utilização em termos tão latos que esta quase passa a poder ser usada… por tudo e por nada;
- Introduz a utilização de drones com câmaras para efeitos de videovigilância por parte das autoridades policiais, sem quaisquer limites ou condições de utilização.
- Introduz cobardemente o reconhecimento facial nos sistemas de videovigilância do espaço público: de forma encapotada, sem qualquer discussão pública, avaliação de impacto ou demonstração de necessidade. Idem para outros tipos de inteligência artificial (IA).
- Legitima o acesso remoto e em tempo real das autoridades a sistemas de videovigilância de qualquer entidade pública ou privada instalados em locais de acesso ao público. Algo que suscita quase tantas questões e dificuldades constitucionais como técnicas, relacionadas com a implementação e segurança dos sistemas.
- Constrange de diversas formas a actuação da Comissão Nacional de Protecção de Dados (CNPD), seja diminuindo prazos, seja retirando competências.

Tudo isto é apresentado como Proposta de Lei à Assembleia da República sem estar acompanhado de um único estudo, avaliação, sumário, opinião, ou sequer alegação de factos que ofereçam qualquer justificação a estas medidas.

Ainda para mais, conhecendo-se agora, por via do parecer junto pela CNPD - que atendendo aos factos lá relatados deveriam ser imediatamente remetidos ao Ministério Público para apuramento de

eventuais responsabilidades criminais - as vergonhosas práticas de videovigilância que têm vindo a ser desenvolvidas em Portugal pela Polícia de Segurança Pública (PSP), Municípios e empresas privadas.

Para cúmulo, tudo isto acontece num contexto em que a anunciada dissolução do Parlamento dá menos de duas semanas para que todo o processo legislativo seja finalizado, o que garante que tudo será feito à pressa, sem ouvir quaisquer entidades, sem realizar consultas públicas, sem haver tempo para estudar devidamente a questão e procurar amplos consensos.

Isto num país considerado dos mais pacíficos do mundo, cujos índices de criminalidade têm consistentemente vindo a decrescer ao longo dos últimos anos e quando Portugal apresenta "os mais baixos índices de criminalidade" desde que há registo.[1]

Do enquadramento legal da videovigilância

A videovigilância, principalmente quando permitida numa escala que possibilita a vigilância massiva dos cidadãos, implica necessariamente uma pesada restrição aos seus direitos fundamentais, em especial o direito à privacidade e o direito à protecção de dados, tal como previstos na Constituição, na Convenção Europeia dos Direitos Humanos e na Carta dos Direitos Fundamentais da União Europeia.

A Convenção Europeia dos Direitos Humanos, no seu artigo 8º e respectiva jurisprudência, diz-nos que a vigilância de um cidadão requer que as autoridades tenham um interesse legítimo e razoável suspeita sobre esse cidadão em particular. Também a Carta dos Direitos Fundamentais da União Europeia, nos seus artigos 7º e 8º, interpretados de acordo com Convenção Europeia dos Direitos Humanos (por via do artigo 52º n.º3 da Carta), e a jurisprudência do Tribunal Europeu dos Direitos Humanos deixam claro o carácter de direito fundamental do direito à privacidade e do direito à protecção de dados pessoais.

A videovigilância do espaço público afecta todas as pessoas, na medida em que o próprio conceito implica a vigilância de qualquer pessoa que circule no espaço público sem que haja uma suspeita razoável sobre cada pessoa que é vigiada, sem que haja genuíno consentimento dessas pessoas, ou sequer um conhecimento informado das concretas práticas de vigilância. Ou seja, uma monitorização geral e indiscriminada das pessoas que por ali passam, como se cada uma delas fosse suspeita ou um potencial criminoso.

A vigilância do espaço público é especialmente gravosa dada a importância deste espaço para a vida pública-social. Os cidadãos podem sempre escolher não frequentar espaços privados que imponham videovigilância, mas não podem escolher não sair à rua.

1 Ministro da Administração Interna, 2021-03-30 https://tvi24.iol.pt/sociedade/eduardo-cabrita/portugal-regista-os-mais-baixos-indices-de-criminalidade-desde-que-ha-registo

Da falta de demonstração da necessidade

A presente Proposta de Lei, aparentemente alheada daquele que é o regime constitucional vigente em termos da restrição de direitos fundamentais, é apresentada sem qualquer estudo prévio ou avaliação, opinião ou sequer uma singela alegação de factos que possam justificar as medidas que são apresentadas.

De igual forma não são apresentados dados que demonstrem a eficácia de cada uma das medidas ora propostas para a redução da criminalidade, e muito menos foi avaliada a eficácia das medidas já existentes.

Na sua Exposição de Motivos, no que respeita à demonstração da necessidade destas medidas, diz-se somente que:

> *"Volvidos 15 anos, (…) os avanços tecnológicos, que motivaram alterações significativas no que diz respeito às características técnicas dos sistemas que o mercado oferece em cada momento, exigem que o quadro legal seja adaptado às soluções técnicas hoje existentes".*

Ou seja, a Proposta de Lei atesta a sua inconstitucionalidade logo na exposição de motivos. Confessa que não existe de facto qualquer motivo que imponha a necessidade de tomar medidas que são bastante mais gravosas para os direitos fundamentais dos cidadãos. Na verdade, diz-se claramente que o que motiva a alteração legislativa proposta são as "alterações das características técnicas dos sistemas disponíveis no mercado". Considera portanto que é o quadro legal que tem de ser modificado de forma a permitir as soluções técnicas hoje existentes no mercado - sem qualquer consideração pelos seus efeitos dessas novas tecnologias nos direitos fundamentais de quem é vigiado. Ou seja, a proposta de lei quer banalizar a utilização de câmaras de videovigilância e introduzir drones, reconhecimento facial, inteligência artificial, etc., não porque seja de facto necessário usar essas tecnologias para os fins prosseguidos pela videovigilância, mas simplesmente porque essa tecnologia existe no mercado.

Tal não deixa de ser uma curiosa interpretação e aplicação do princípio da proporcionalidade, nomeadamente porque significa a sua total obliteração.

Em suma, na exposição de motivos da Proposta de Lei não é alegada qualquer justificação válida para as alterações legais propostas. A presente proposta vem fundamentada em puro achismo e paranóia securitária.

Das mudanças legislativas e do alargamento dos fins admissíveis para a videovigilância

A presente Proposta de Lei, no seu artigo 3º, alarga de tal forma os fins que permitem o recurso a videovigilância, que esta perde o seu carácter de utilização excepcional - na estrita medida do necessário - que tinha até agora. Tal acontece quer através da remissão para os fins expressos na Lei

da Segurança Interna, quer através da introdução de novas alíneas que recorrem a conceitos indeterminados que podem ser livremente abusados: “operações policiais complexas”, “elevada circulação ou concentração de pessoas”, “prevenção de actos terroristas”, “resposta operacional a incidentes de segurança”, etc. Com tão amplo regime, quase seria possível, por exemplo, ter câmaras em toda e cada uma das ruas das cidades de Lisboa e Porto. Será esse o objectivo?

No mesmo sentido, o artigo 4º, parece querer restringir a aplicação do princípio da proporcionalidade ao seu sub-princípio da adequação. No regime actual, "é autorizada a utilização de câmaras de vídeo quando tal meio se mostre **concretamente o mais adequado** para a manutenção da segurança e ordem públicas e para a prevenção da prática de crimes. Na proposta apresentada, basta que o meio mostre **ser adequado** (e não o mais adequado) a “qualquer dos fins do artigo anterior” (que, como veremos, são bastante mais latos).

Também a alínea que estipulava que “a autorização de utilização de câmaras de vídeo pressupõe sempre a existência de riscos objetivos para a segurança e a ordem públicas” foi simplesmente suprimida.

Foi ainda suprimida a proibição expressa de captura de conversas de natureza privada.

Quadro comparativo:

Tema	Lei actual	Proposta
Utilização pressupõe riscos objectivos?	“a autorização de utilização de câmaras de vídeo pressupõe sempre a existência de riscos objetivos para a segurança e a ordem públicas”	(suprimido)
Devem ser antes consideradas alternativas menos lesivas?	É autorizada a utilização de câmaras de vídeo quando tal meio se mostre concretamente **o mais adequado** para a **manutenção da segurança e ordem públicas e para a prevenção da prática de crimes**, tendo em conta as circunstâncias concretas do local a *vigiar*.	É autorizada a utilização de câmaras de vídeo quando tal meio **se mostre adequado** para os **fins previstos no artigo anterior**, tendo em conta as circunstâncias concretas do local *a proteger*
Proibição de captura de conversas privadas	É igualmente vedada a captação de imagens e sons (…) quando essa captação afete, de forma direta e imediata, a intimidade das pessoas, **ou resulte na gravação de conversas de natureza privada**.	É igualmente vedada a captação de imagens e sons quando essa captação afete, de forma direta e imediata, a esfera da reserva da vida íntima e privada.

No que respeita aos fins permitidos e aos meios que podem ser utilizados, como bem refere a CNPD, não existe qualquer limitação intrínseca a cada um dos meios, os quais variam consideravelmente no grau de afectação de direitos dos cidadãos. Um drone equipado com câmara, por exemplo, tem um potencial de afectação de direitos enormemente superior ao de uma câmara

fixa. Prevê-se apenas uma ponderação caso a caso, em vez de limitações concretas à utilização de cada meio. Também por aqui é violado o princípio da proporcionalidade.

Transversal a todo o diploma está a ideia que a mera videovigilância, só por si, não é susceptível de afectar os direitos dos cidadãos. Como se a videovigilância dos cidadãos só ganhasse relevância jurídica no momento em que as imagens sejam gravadas e a gravação seja acedida. Nesta lógica, propõe-se, por exemplo:

- captação de imagens sem gravação, incluindo as captadas por drones, "exclusivamente para efeitos de visualização" (art. 17º) - dispensando-se assim o normal pedido de autorização (arts. 5º a 7º).
- utilização de câmaras portáteis e drones sem tais procedimentos e sem sequer existir um pedido prévio de autorização (art. 10º/5), quando este não puder ser pedido "em tempo útil" (sendo que mesmo autorização a posteriori passa a ser da competência da tutela em vez da competência da CNPD, como actualmente).
- permissão de recolha de dados biométricos, mas limitação do tratamento desses dados para fins de combate ao terrorismo (n.º 2 e 3 do art. 18º/2).

A videovigilância consiste sempre numa restrição de direitos fundamentais que ocorre em dois momentos distintos: no momento da recolha e no momento de um eventual acesso posterior à gravação. Em ambos os momentos deve ser verificada a proporcionalidade na restrição de direitos fundamentais.

Obviamente, a recolha de dados biométricos envolve necessariamente o tratamento de dados biométricos, pelo que distinção traçada na proposta de lei carece de qualquer lógica.

E não é por o acesso aos dados biométricos recolhidos ser apenas permitido para fins de combate ao terrorismo que isso não implica uma recolha generalizada e indiscriminada de dados biométricos de todas as pessoas. Os fins não justificam os meios. Principalmente quando se prevê que tal possa ser feito com recurso a drones e com tratamento automatizado de dados por programas de inteligência artificial, nomeadamente de reconhecimento facial.

De igual forma, a mera captação de imagens, mesmo que apenas para efeitos de visualização, já por si afecta os direitos fundamentais das pessoas que são vigiadas. A gravação e posterior acesso a essas imagens apenas gera um novo dano. Logo, mesmo a mera captura de imagens sem gravação tem necessariamente de cumprir exigências de proporcionalidade, não podendo beneficiar de um regime de isenção das normais regras e condições utilização previstas. Aliás, tal certamente apenas fará com que o "não haver tempo útil" para o pedido se torne a regra, dada a simplificação do regime - é portanto um incentivo a más práticas.

Da utilização de drones equipados com câmaras de videovigilância

No que respeita em especial à utilização de drones, propõe-se a equiparação destes dispositivos a meras câmaras portáteis, aplicando-se-lhes o regime destas. Como se drones fossem sequer comparáveis às câmaras portáteis utilizadas até agora, cuja única diferença para as câmaras fixas é a susceptibilidade de serem rapidamente relocalizadas para um novo local, i.e., a portabilidade.

Não deveria ser necessário referir que os impactos da utilização de drones nos direitos dos cidadãos é de toda uma outra ordem de grandeza. Drones são capazes de cobrir áreas gigantescas, em vez de estarem confinados a uma área definida. Em drones não é possível colocar "máscaras de privacidade" que impeçam que espaços privados e reservados (por exemplo espaços ao livre dentro de casas) sejam gravados, tal como é requerido para videovigilância na via pública. Ao contrário de câmaras fixas, que são claramente indicadas ao público, quer pela sua sinalização, quer pela sua presença física, os cidadãos não se apercebem quando estão a ser vigiados por drones.

Perante todos estes riscos, o que se propõe na proposta de lei? Isentar a utilização de drones das medidas de divulgação e informação ao público sobre tal utilização, e da necessidade de identificar eventuais dados biométricos recolhidos. (Vide arts. 10º/3, 24º e 25º)

Drones de videovigilância podem ter uma fenomenal capacidade de captura de imagem e som. São portanto potenciais fontes de gravíssimas violações de direitos fundamentais. É dessa forma que devem ser encarados, e não como meros novos brinquedos tecnológicos ao dispor discricionário das forças policiais.

Da utilização de sistemas de inteligência artificial em sistemas de videovigilância

A presente Proposta de lei abre a porta, da forma mais cobarde possível, à utilização de mecanismos de inteligência artificial em sistemas de videovigilância do espaço público: sem qualquer debate público prévio, sem consultas públicas sobre o tema, sem sequer ter sido ouvida previamente a CNPD. Discretamente é acrescentado um artigo que menciona tal possibilidade, sem sequer regular a sua utilização.

No artigo 18º, volta-se a repetir as supra referidas confusões conceptuais, ao referir-se "visualização e o tratamento", como se a visualização não consistisse em tratamento de dados; e ao permitir-se a captura de dados biométricos mas limitar-se o seu tratamento aos fins de combate ao terrorismo, mais uma vez: como se a captura de dados biométricos não consistisse em tratamento de dados.

Prevê-se a utilização de um "sistema de gestão analítica dos dados captados" - o que quer que isso signifique. Por fim, parece que no n.º 5 se admite tacitamente a possibilidade de utilização de inteligência artificial. Como bem aponta a CNPD, a Proposta de Lei não se digna sequer a consagrar

uma expressa permissão da utilização de inteligência artificial, somente mencionando tal expressão de forma quase acidental. E a expressão "reconhecimento facial" então nem sequer é utilizada.

Ora, mencionar não é regular. Em lado algum se regula a utilização destas tecnologias. Que regras e critérios seguirá a sua utilização? Esta é a questão-chave para aferir da proporcionalidade da restrição de direitos que se visa efectuar, e logo, da possibilidade da sua utilização à luz da Constituição. Infelizmente, a lei é omissa. Salvo no que respeita aos "sistemas de gestão analítica" de dados. Para estes, prevê-se a "aplicação de critérios técnicos de acordo com os fins a que se destinam". Mais uma vez: o que quer que isso signifique. "Aplicação de critérios técnicos" é uma expressão absolutamente vazia de conteúdo, que pretende passar por regulação quando significa precisamente a ausência de regulação.

A banalização da videovigilância, agravada com a utilização de "sistemas analíticos", "dados biométricos" e "inteligência artificial", leva a práticas de vigilância massiva da população.

Por essa razão, muitas têm sido as vozes a alertar para os perigos que tais tecnologias levantam quando aplicadas à vigilância do espaço público. A título de exemplo, a autoridade de protecção de dados italiana (Garante Per La Protezione Dei Dati Personali) confirmou recentemente[2] que a utilização de reconhecimento facial em espaços públicos constitui uma prática de vigilância massiva:

> *«De acordo com a posição tomada pelo Conselho da Europa, a Autoridade de Protecção de Dados considera que a utilização do reconhecimento facial para efeitos de prevenção e supressão do crime é altamente problemática. Em particular, deve ser tido em conta que o sistema Sari Real Time permitiria actividades de tratamento automatizado em larga escala que poderiam também dizer respeito a indivíduos que participam em eventos políticos e sociais.»*

Como bem sabemos, Portugal já deu dos piores exemplos na Europa no que respeita ao tratamentos de dados pessoais de indivíduos que participam em eventos políticos e sociais, nomeadamente manifestações políticas. Dessa forma, deveria seriamente reconsiderar o tratamento automatizado e em larga escala desse tipo de dados, naturalmente bastante mais problemático que o tratamento não automatizado nem em larga escala que existe actualmente.

Como bem refere a autoridade italiana, a utilização do reconhecimento facial para efeitos de prevenção e supressão do crime é altamente problemática. E isto acontece mesmo que a videovigilância e recolha de dados biométricos tenha um propósito específico, como seja procurar pessoas específicas ou prevenir actos terroristas. Como vimos supra, mesmo que a consulta posterior dos dados seja sujeita a limitações (como o combate ao terrorismo), continua a ter de se recolher os dados biométricos de todas as pessoas que passarem em determinado local, e isso já basta para colocar em causa os direitos fundamentais dessas pessoas.

2 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575842

De acordo com a Autoridade Europeia para a Proteção de Dados (AEPD) e o Comité Europeu para a Proteção de Dados (CEPD), os dados pessoais e a privacidade de qualquer pessoa que passe no espaço vigiado são indevidamente infringidos por tal vigilância[3]:

> *Tendo em conta os riscos extremamente elevados colocados pela identificação biométrica remota de indivíduos em espaços acessíveis ao público, a AEPD e o CEPD apelam a uma proibição geral de qualquer utilização de IA para reconhecimento automático de características humanas em espaços acessíveis ao público, tais como reconhecimento de rostos, marcha, impressões digitais, ADN, voz, teclas e outros sinais biométricos ou comportamentais, em qualquer contexto.*

Muito recentemente, o Parlamento Europeu aprovou um relatório[4] que defende a proibição da vigilância biométrica massiva[5]. O relatório insta a Comissão Europeia a implementar "uma proibição de qualquer processamento de dados biométricos, incluindo imagens faciais, para fins de aplicação da lei que conduza à vigilância de massas em espaços acessíveis ao público". Apela também a "uma moratória sobre a implantação de sistemas de reconhecimento facial para fins de aplicação da lei que tenham a função de identificação", juntamente com a "proibição permanente da utilização de análise e/ou reconhecimento automático em espaços acessíveis ao público de outras características humanas, tais como o andar, impressões digitais, ADN, voz e outros sinais biométricos e comportamentais".

Convém ter presente que a interferência nos direitos fundamentais à privacidade e à protecção de dados pessoais provocada pela vigilância biométrica é agravada pelo facto de esta exigir o tratamento de formas de dados especialmente sensíveis. Os dados biométricos das pessoas, tais como os seus rostos, são centrais para a sua identidade pessoal. Além disso, os dados pessoais relacionados com as características físicas, fisiológicas ou comportamentais permitem a identificação única de uma pessoa.

O seu tratamento pode, portanto, violar os direitos das pessoas à dignidade, o seu direito à igualdade e à não discriminação, à autonomia e à autodeterminação. Isto não é negativo apenas para indivíduos, mas também para comunidades. Muitos grupos europeus e internacionais de direitos humanos têm chamado a atenção para muitos outros danos graves que a vigilância biométrica massiva implica, incluindo os direitos à livre associação, reunião, expressão e pensamento, e direitos a um processo justo, procedimento adequado e boa administração.

Há precisamente dois meses, o Alto Comissário das Nações Unidas para os Direitos Humanos pronunciou-se contra a vigilância biométrica massiva[6] nos seguintes termos:

> *«O reconhecimento biométrico remoto está ligado a uma profunda interferência com o direito à privacidade. A informação biométrica de uma pessoa constitui um dos*

3 https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en
4 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf
5 https://edri.org/our-work/celebrating-a-strong-european-parliament-stance-on-ai-in-law-enforcement/
6 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E

> *atributos chave da sua personalidade, uma vez que revela características únicas que a distinguem de outras pessoas. Além disso, o reconhecimento biométrico à distância aumenta dramaticamente a capacidade das autoridades estatais de identificar e seguir sistematicamente os indivíduos em espaços públicos, minando a capacidade das pessoas de se deslocarem sem serem observadas e resultando num efeito negativo directo no exercício dos direitos à liberdade de expressão, de reunião pacífica e de associação, bem como à liberdade de movimento. Neste contexto, o Alto Comissário congratula-se, portanto, com os recentes esforços para limitar ou proibir a utilização de tecnologias de reconhecimento biométrico em tempo real.»*

Em discussão actualmente na União Europeia, o Artificial Intelligence Act[7], a proposta europeia para a regulação da inteligência artificial vem propor a proibição de utilização de sistemas de identificação biométrica em tempo real por parte de autoridades policiais.

Pelo contrário, a presente proposta de lei, no seu art. 16º, consagra o acesso em tempo real, de forma presencial ou remota, a sistemas de videovigilância de qualquer entidade pública ou privada, instalados em locais públicos ou privados de acesso ao público. Tal suscita quase tantas questões e dificuldades constitucionais como técnicas, relacionadas com a implementação e segurança dos sistemas, porquanto implica ligar os sistemas de CCTV através da Internet, com todas as implicações de segurança que isso acarreta.

Por fim, está por esclarecer quem iria gerir, e sob que regras iria funcionar, a base de dados biométricos centralizada dos dados biométricos recolhidos.

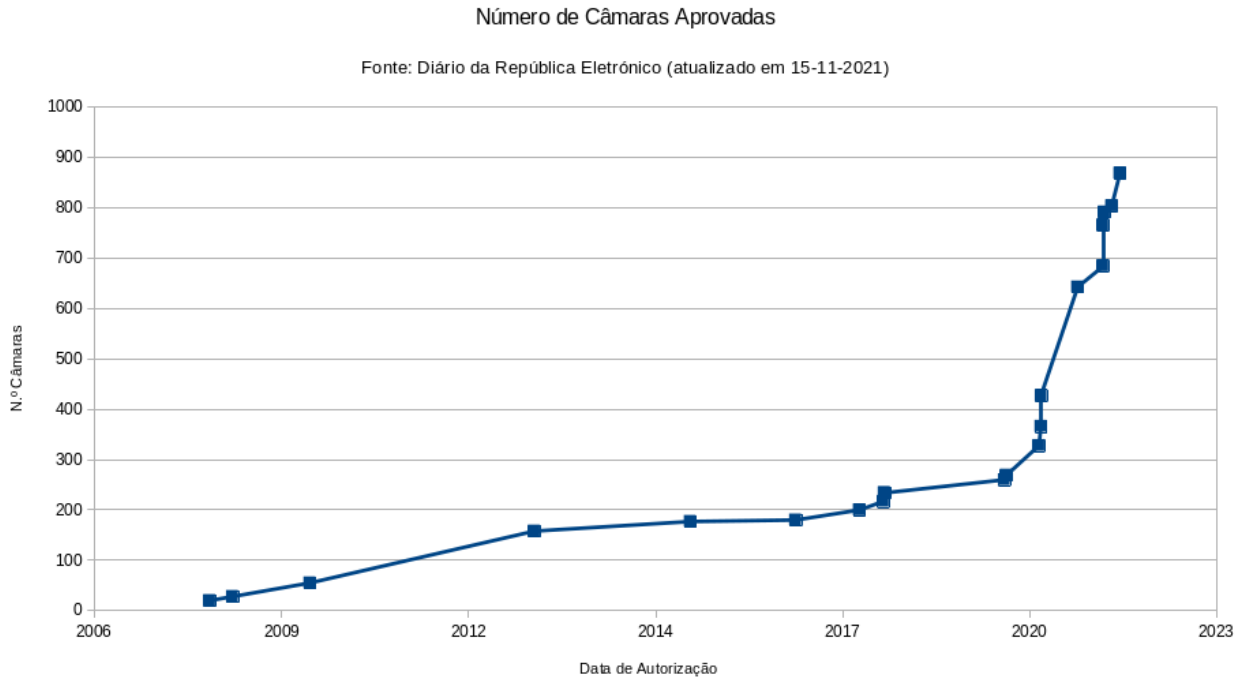
Desde modo, torna-se evidente que, com a aprovação desta proposta de lei, Portugal entraria em contra-corrente com as principais autoridades na matéria e com as actuais tendências legislativas.

Do manietar da CNPD ao crescimento exponencial da videovigilância

Desde a Lei n.º 9/2012 que se tem vindo progressivamente a limitar seriamente a possibilidade de a CNPD agir como a autoridade de protecção de dados dos cidadãos portugueses. Desde tal alteração legislativa que a CNPD está impedida de se pronunciar sobre a proporcionalidade da utilização de meios de videovigilância do espaço público. Tal competência passou para o Ministério que tutela as forças de segurança. Como seria expectável, o Ministério da Administração Interna não tem qualquer vontade - e a julgar pelos consecutivos chumbos recentes dos pedidos de autorização à CNPD que implicavam utilização de sistemas inteligência artificial – competência, para efectuar juízos de ponderação da proporcionalidade ou sequer realizar avaliações de impacto. Na verdade, não há qualquer entidade que realize o necessário juízo de ponderação da proporcionalidade da expansão da videovigilância. O Ministério da Administração Interna tem uma visão acrítica, aceitando todos os pedidos, e mais quantos houvesse.

7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

O resultado foi o crescimento significativo do número de câmaras de videovigilância em Portugal, tendo nos últimos anos sido agravado e entrado em crescimento exponencial. A continuar a este ritmo, pouco faltará para que haja uma câmara em cada esquina.



Hoje em dia, a avaliação da CNPD está essencialmente[8] limitada a meros pormenores técnicos relacionados com a instalação, segurança e integridade dos sistemas. Ainda que, no discurso público, se continue a abusar do argumento de que "foi autorizado da CNPD" como forma de dar a entender aos mais incautos de que houve de facto uma entidade de fiscalização idónea, reputada e independente a controlar a decisão.

Mas agora, mesmo essa autorização limitada deixa de existir. A autorização é transformada em mero parecer não vinculativo. Para isto mais valia renomear aquela que deveria ser a nossa Autoridade[9] de protecção de dados pessoais (que continua com o desígnio de "Comissão") como "Consultora da Instalação, Segurança, Integridade e Outras Tecnicalidades do Tratamento dos Dados".

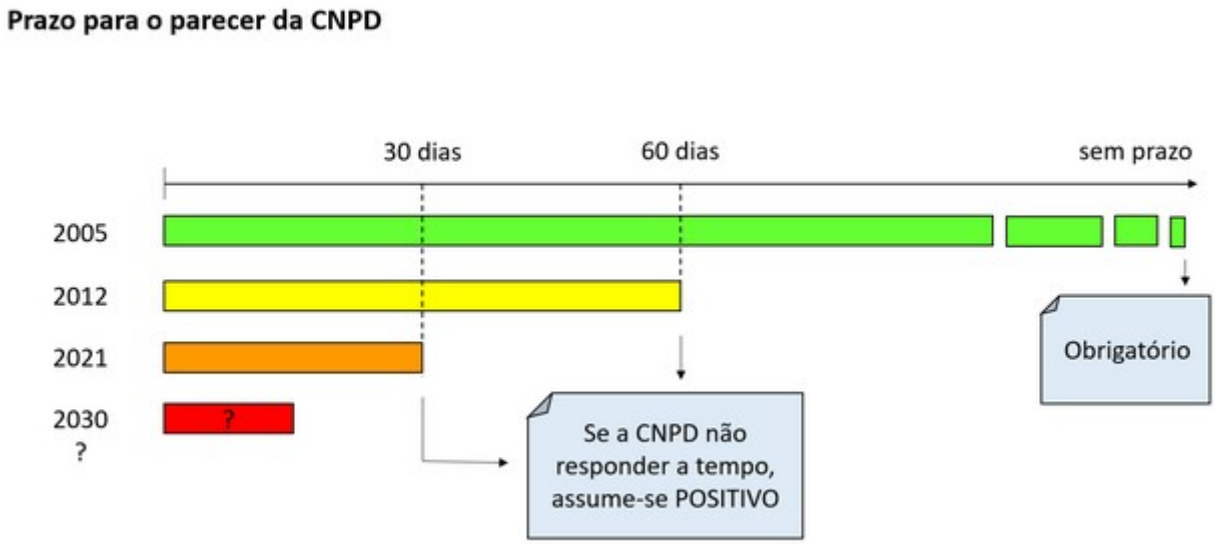
É que de Autoridade e de Protecção de Dados resta já muito pouco.

Mas a Proposta de Lei não se fica por aqui. Leva ainda mais longe a tentativa de maniatação da CNPD. Sendo publicamente conhecidas as dificuldades e constrangimentos económicos[10] que limitam a acção da CNPD, propõe o Governo (que é em última análise responsável por tais

8 Excepção feita quando se trata de videogivilância que em concreto incida em locais que devam ser usados com resguardo (praias), interiores de casas ou a intimidade da vida das pessoas.
9 Expressão usada pelo Regulamento Geral de Protecção de Dados
10 https://eco.sapo.pt/2018/05/16/presidente-da-protecao-de-dados-diz-que-nao-tem-dinheiro-para-salarios-em-junho-muito-menos-para-fiscalizar-nova-lei/

constrangimentos) a redução do prazo para a emissão do parecer, de 60 para 30 dias. Pior: se a CNPD não conseguir responder em tempo útil, o parecer considera-se positivo. No entender do Ministério Público, no parecer que juntou, tal pode configurar uma inconstitucionalidade.

Vejamos a evolução legislativa:



Primeiro era uma autorização obrigatória com um necessário juízo de proporcionalidade e sem prazo, depois reduziu-se o escopo da autorização, depois reduziu-se o prazo a 60 dias, e agora quer-se torná-lo não vinculativo e com ainda menos prazo, sendo considerado positivo caso não haja resposta (n.º 4 artigo 5.º).

Em sentido contrário vai o crescimento do tempo de duração de cada autorização.

Primeiro era um regime excepcional, apenas usado quando demonstradamente necessário. Agora, pretende-se a liberalização da utilização e o prazo, que originariamente era de um ano, passa a ser de cinco anos (n.º 3 artigo 7.º).

A continuação deste maniatar da CNPD é notória em várias normas do diploma. Além dos pontos já referidos supra, nas respectivas secções (consulta prévia - art. 9º, ou os protocolos especiais do art. 10º e 17º), repare-se na estranha consagração da Inspecção-Geral da Administração Interna (IGAI) como a entidade competente para "emitir recomendações que visem a melhoria dos procedimentos de recolha e tratamento de dados pessoais, através dos sistemas de videovigilância" (art. 23.º/2). Não se compreende se tal norma visa criar redundâncias entre diferentes entidades no que respeita a tal avaliação, ou se visa de facto retirar tal competência à CNPD, procurando uma nova autoridade de protecção de dados, porventura mais simpática, na figura da IGAI.

Também de forma original, o art. 26.º parece limitar a actuação da CNPD enquanto entidade fiscalizadora. Limita-se, nomeadamente, as formas como pode a CNPD exercer os seus poderes de fiscalização: somente através "inspeções periódicas por amostragem". Já na fiscalização dos dados recolhidos, restringe-se o acesso da CNPD a esses dados aos casos em que ocorra "denúncia ou suspeita fundamentada da sua recolha ilegítima".

Da demonstrada incapacidade de proteger as gravações

Segundo o parecer junto pela CNPD, foram detetadas graves situações de falha na proteção das gravações e registo dos acessos e integridade dos mesmos. Aliás, o conteúdo do parecer é de tal forma grave que este deve ser remetido ao Ministério Público para apuramento de eventuais responsabilidades criminais. Se isto é o que acontece nos sistemas de videovigilância inspecionados pela CNPD com os seus escassos meios, não há como não questionar o estado de todos os restantes sistemas ainda não fiscalizados.

A Proposta de Lei, ao agilizar ainda mais o processo de instalação de videovigilância e a aliviar as exigências de fiscalização estará, nestas circunstâncias, a contribuir implicitamente para o aumento do risco de acessos indevidos às imagens e conversas que as pessoas possam ter nas ruas. Tal contraria o próprio propósito da lei de proteger pessoas, criando em vez disso novos riscos de segurança. Segundo o parecer da CNPD, as forças policiais não se encontram em condições de garantir a adequada proteção dos dados.

Do timing

Tudo isto acontece num contexto de manifesta falta de legitimidade política (em sentido não jurídico) para a aprovação destas medidas, dada a anunciada dissolução eminente da Assembleia da República.

A prossecução do presente processo legislativo, quando faltam apenas duas semanas para dissolução da Assembleia e o diploma ainda nem foi discutido em Comissão, não existem propostas de alteração disponíveis, e tendo ainda de ir a plenário para votação final global, transparece a assunção e/ou conformação com o factro de que se pretende levar à aprovação um diploma tão

problemático como este, numa área especialmente sensível para os direitos fundamentais dos cidadãos, quando:

- Não houve uma necessária discussão pública
- Não foi realizada qualquer consulta pública
- Não foram ouvidas no Parlamento quaisquer entidades
- Não foram juntos quaisquer documentos que demonstrem a eficácia ou necessidade

Tudo isto, num cenário em que não haverá tempo para suprir estas lacunas, e a pressão do tempo fará com que tudo seja feita à pressa.

Do efeito da videovigilância

Apresentada como uma solução tecnológica para qualquer tipo de crime, a videovigilância é promovida politicamente passando a ideia de segurança. Mas como a CNPD demonstra no seu parecer, verifica-se que *«[…]a utilização dos sistemas de videovigilância não cumpre as regras relativas à segurança e integridade dos tratamentos de dados pessoais»*. Criar uma sensação de segurança (para alguns) sem dar garantias de que de facto o indivíduo está mais seguro, oferece apenas uma sensação de segurança que é falsa, sendo porventura pior que não ter videovigilância de todo, já que pelo menos nesse caso uma pessoa não assume nem adapta o seu comportamento como se estivesse numa situação de segurança quando na verdade não está.

Estar sob vigilância permanente afecta o indivíduo, que consciente ou inconscientemente, altera o seu comportamento, independentemente de estar ou não a cometer um crime ou infração. A videovigilância massiva do espaço público resulta numa sociedade mais conformista. Resulta numa sociedade menos disposta a sair fora da norma e a desafiar o *status quo*, pois tudo é vigiado. A sensação de poder estar a ser vigiado a todo o momento, e de que poderão haver repercussões para qualquer comportamento desviante, em última análise não inibe apenas a prática de crimes. Inibe o ser social e político que é o ser humano.

Conclusão

A Segurança é um valor fundamental, mas não é alcançada com uma câmara em cada esquina.
A Segurança é alcançada, antes de tudo, com melhores políticas sociais.
A Segurança é alcançada com apropriados recursos financeiros e humanos nas forças políciais, que há muito escasseiam[11] [12] [13]. Curioso como tais restrições orçamentais rapidamente desaparecem quando há brinquedos tecnológicos envolvidos e grandes contratos em vista.

A videovigilância do espaço público, quando sujeita a um regime legal permissivo que incentiva a vigilância massiva dos cidadãos, agravada pela utilização desregulada de drones e sistemas de inteligência artificial, é uma grave restrição a direitos fundamentais de todos os cidadãos.

Contudo, a presente Proposta de Lei não realiza qualquer juízo de ponderação da proporcionalidade destas medidas, nem demonstra ou sequer alega a sua necessidade. O que aliás corresponde a uma postura que vem de longe, no que respeita à videovigilânca em Portugal, cuja implementação é constantemente realizada com ausência de qualquer tipo de fundamento:

> *«O PÚBLICO pediu à PSP acesso a alguns pareceres da direcção nacional que justificam os pedidos, mas tal foi recusado por "razões de segurança e de sigilo profissional", e também questionou sobre a existência de relatórios sobre a consequência da videovigilância na redução da criminalidade, porém a PSP respondeu que os "dados não são públicos".»*[14]

Não se trata de uma mera questão menor, no procedimento legislativo, como que um mero esquecimento da junção da necessária documentação. Trata-se de uma total ausência de fundamentação. De facto, na fundamentação da Proposta de Lei, nada existe que que não seja puro achismo e paranóia securitária.

Por outras palavras, a Proposta de Lei não cumpre as exigências constitucionais na restrição de direitos fundamentais – nem sequer tenta cumprir – revelando um total desprezo e/ou alheamento do quadro constitucional em vigor.

---

11 **"(há) uma inoperacionalidade gritante por falta de meios"** - António Sousa, Sindicato Nacional da Carreira de Chefes da PSP - https://www.publico.pt/2017/04/19/sociedade/noticia/chefes-da-psp-alertam-para-falta-de-meios-e-envelhecimento-do-efectivo-1769334

12 **"há verdadeiramente falta de recursos"** – Carlos Moedas, Presidente da C.M. Lisboa - https://www.publico.pt/2021/10/26/local/noticia/moedas-preocupado-inseguranca-lisboa-1982562

13 **"A Polícia de Segurança Pública não tem efectivos suficientes nem condições"** – Rui Moreira, Presidente da C.M. Porto. https://www.publico.pt/2017/04/19/sociedade/noticia/chefes-da-psp-alertam-para-falta-de-meios-e-envelhecimento-do-efectivo-1769334

14 https://www.publico.pt/2021/09/20/politica/noticia/desde-2013-videovigilancia-rua-passou-38-850-camaras-autorizadas-1978004

As claras inconstitucionalidades fazem com esta Proposta de Lei esteja morta à nascença. Mesmo que, por hipótese académica, se admitisse a obtenção de uma maioria parlamentar para a sua aprovação na Assembleia da República, seria apenas mais uma lei que iria merecer um pesado chumbo do Tribunal Constitucional[15].

Por não cumprir, de forma gritante, as exigências de um Estado de Direito democrático no que respeita à restrição legislativa de direitos fundamentais, recomenda-se a devolução imediata da presente Proposta de Lei ao Governo.

Associação D3 – Defesa dos Direitos Digitais

16 de Novembro de 2021

15 O que parece estar a tornar-se num hábito, lamentavelmente, em leis que versam sobre tecnologia e direitos.