COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Deliberação n.º 569/2015

1. Introdução

Foram publicadas diversas notícias, em vários órgãos de comunicação social, que indiciavam o acesso indevido a dados pessoais do Primeiro-Ministro relativos à sua situação tributária e contributiva, na posse respetivamente da Autoridade Tributária e Aduaneira (AT) e da Segurança Social (SS).

Indiciando tais acessos a violação das disposições legais em matéria de proteção de dados, designadamente da Lei n.º 67/98, de 26 de outubro (LPD), decidiu a Comissão Nacional de Protecção de Dados (CNPD), no âmbito dos seus poderes de investigação e inquérito previstos na alínea a) do n.º 3 do artigo 22.º da LPD, abrir o presente processo.

A CNPD sublinha que, independentemente da existência de outros eventuais ilícitos decorrentes das situações que subjazem às notícias e dos factos entretanto vindos a público, a averiguação levada a cabo se restringiu exclusivamente a matérias do âmbito das suas competências. Sublinha, ainda, que a presente Deliberação versa apenas sobre os factos averiguados na AT, ficando a matéria relativa aos eventuais acessos na Segurança Social para deliberação autónoma.

*

Foram realizadas as diligências que se reputaram pertinentes para o esclarecimento dos factos, nomeadamente a realização de verificações nos sistemas de informação e a recolha de testemunhos de dirigentes e funcionários da AT, bem como do Presidente do Sindicato dos Trabalhadores dos Impostos.

As diligências efetuadas e os factos apurados encontram-se descritos no Relatório de Inspeção junto aos autos, homologado pela presente deliberação, da qual faz parte integrante.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Assim sendo, enunciam-se aqui de forma sintética os factos mais relevantes, e que estão desenvolvidos e comprovados no Relatório de Inspeção, para suportar a apreciação e as conclusões desta deliberação.

2. Principais factos apurados

a) Política de segurança da AT

Existe um documento denominado "Política de segurança" e uma "Carta de Princípios", sem data, mas anteriores à reestruturação que originou a criação da AT. Encontra-se na sua primeira versão e incide, designadamente, sobre segurança da informação, política de utilização dos recursos informáticos (*v.g.,* correio eletrónico e acesso à Internet), gestão do acesso dos utilizadores.

Estes dois documentos são genéricos e não foram objeto de regulamentação específica, que permita implementar essa mesma política, nem foram acompanhados do desenvolvimento de boas práticas.

b) Gestão dos acessos aos sistemas de informação

Sobre a forma como é realizado e gerido o acesso aos sistemas de informação da AT, resulta essencialmente o seguinte:

- Há uma aplicação específica (Sistema de Gestão de Utilizadores – SGU) para a gestão de utilizadores dos sistemas de informação da AT;
- Em cada serviço e de acordo com a sua "área de negócio", há um responsável local que tem poderes para criar, alterar ou eliminar utilizadores e para atribuir os perfis de acesso;
- Existem regras escritas para a composição da palavra-passe no manual de Política de Segurança da AT;
- Há procedimentos estabelecidos para a forma como os utilizadores são credenciados e para a gestão das contas de utilizadores;
- O universo total de utilizadores internos é de, pelo menos, 12.156;

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- O perfil básico permite que um número alargado de utilizadores conheça a situação contributiva de qualquer cidadão, designadamente as suas declarações de rendimento, estando nestas circunstâncias 9.298 utilizadores com este tipo de permissão de acesso (direções de finanças: 1.935; serviços centrais: 1.834; serviços de finanças: 4.515; serviços aduaneiros: 1.014);
- Há ainda 2.302 utilizadores externos[1] com os mesmos níveis de permissão;

c) Rastreamento das operações realizadas pelos utilizadores

As operações realizadas pelos utilizadores, tais como a consulta, a alteração ou a impressão de informação, são registadas em *logs*. No entanto, não há uma política de análise de *logs* por parte da AT nem está estabelecido um prazo de conservação para a sua manutenção, estando o seu armazenamento dependente do espaço em disco. Assim, a conservação dos *logs* de acesso aos sistemas pode mediar entre um e dois anos.
Verificou-se ainda não existirem mecanismos preventivos aptos a limitar os acessos à informação, no respeito pelo princípio da necessidade.

d) Formação dos dirigentes e funcionários da AT

Só no último ano foi decidido pela AT dar maior importância à formação dos seus dirigentes e funcionários, com incidência específica na proteção dos dados pessoais dos contribuintes e na segurança da informação, através da elaboração de planos de formação nestas áreas e que, entretanto, já este ano, estão a ser executados.

e) Informalidade de procedimentos

Verificou-se que o responsável pela Área de Segurança Informática (ASI) e a coordenadora da Área de Gestão de Impostos, a desempenhar funções de

[1] No conceito de utilizadores externos integram-se, de acordo com o declarado, tarefeiros nos serviços de finanças, estagiários, equipas de desenvolvimento e manutenção em regime de subcontratação, Administradores de Bases de Dados (DBAs) e ainda funcionários da AT a prestar serviço num segundo local.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Subdiretora Geral de Sistemas de Informação (SDGSI) mantêm um reduzido grau de formalização de procedimentos, em especial no que diz respeito aos pedidos para identificação dos funcionários que acederam aos dados fiscais de certos contribuintes – ausência de solicitação escrita, recurso ao meio de comunicação telefónico e entrega de documentos em mão, sem o correspondente registo –, atendendo em particular à possibilidade de estes dados serem utilizados para procedimento disciplinar ou criminal.

Apurou-se igualmente que nem todos os utilizadores que acederam aos dados fiscais do Primeiro-Ministro e do Presidente da República foram objeto de reporte à Direção dos Serviços de Auditoria Interna (DSAI).

f) Sistema de alarmística – "Lista VIP"

Em 30 de setembro de 2014, o responsável pela ASI elaborou uma proposta, denominada "Controlo do Acesso aos Dados – alarmística em caso de consulta/alteração de dados sensíveis", que consistia na configuração de alertas a serem espoletadas em caso de «verificação de consulta ou alteração de dados de determinados contribuintes que, na ausência de melhor conceito, denominamos VIP». Para tal, considerava-se «indispensável a identificação dos NIFs que ficarão sobre monitorização, sugerindo-se que, numa fase inicial, se incluam, pelo menos, os principais titulares dos órgãos de soberania». A proposta adiantava o procedimento a seguir em caso de ocorrência de acesso.

Em troca de correspondência posterior com a DSAI, a ASI afirma, em 24 de outubro de 2014, que «[...] o início do processo está apenas dependente da indicação à ASI dos NIFs que serão objeto de alerta, salientando que [q]uando refiro ASI quero dizer apenas os funcionários que têm como tarefa obter este tipo de informação (neste momento sou apenas eu) [...]».
Ainda na mesma data, o Diretor da DSAI emite ordem de serviço a abrir processo geral para a alarmística.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

No decurso do mês de novembro, por duas vezes, foi comunicado à DSAI terem ocorrido acessos a informações fiscais de alguns contribuintes. Assim, o responsável pela ASI remeteu ao Diretor da DSAI um *e-mail* «a comunicar o resultado dos alertas de segurança que temos implementados para as operações de consulta/alterações», em relação aos Números de Identificação Fiscal (NIFs) do Primeiro-Ministro e do Presidente da República, respetivamente em 6 e 28 de novembro. Em ambas as comunicações, eram identificados os funcionários que acederam, os serviços de finanças onde trabalham, data e hora da consulta.

Estas duas comunicações, que seguiram em cópia para o Gabinete da SDGSI, foram juntas ao processo de auditoria relativo à alarmística e foram objeto de instrução.

No dia 18 de fevereiro de 2015, a DSAI solicitou à ASI a informação sobre os critérios de constituição do grupo de contribuintes a monitorizar, «denominados de "VIP"», assim como a sua identificação e se houve alterações nesse universo. A resposta veio no dia 24 de fevereiro de 2015, após insistência, informando qual o «universo sujeito a alerta VIP», pelo que elenca quatro nomes e respetivos NIFs («Passos Coelho», «Cavaco Silva», «Paulo Portas», «Paulo Núncio»), indicando que os três primeiros nomes estão inseridos desde o início e o último foi incluído na sequência de processo de auditoria por consulta aos dados fiscais do Secretário de Estado dos Assuntos Fiscais (SEAF). Afirma ainda aguardar «indicação sobre qual o universo a abranger», mas não especifica de quem.

Verifica-se, todavia, que no dia anterior a esta resposta, a 23 de fevereiro de 2015, o Diretor Geral (DG) da AT, António Brigas Afonso, já tinha revogado o procedimento de alarmística, tendo o despacho do DG sido comunicado pessoalmente na mesma data ao responsável da ASI.

Apurou-se igualmente que não corria nem nunca correu termos na DSAI qualquer processo de auditoria por consulta aos dados fiscais do SEAF.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

3. Apreciação

3.1 Ausência de regulação dos tratamentos de dados pessoais da AT

Importa, em primeiro lugar, notar que não existe legislação que regule especificamente o tratamento de dados pessoais da AT. Este tratamentos, por regra, refletem as determinações do legislador quanto à matéria fiscal, sendo criados pela AT para cumprir objetivos previstos em normas legais – frequentemente nas leis orçamentais –, as quais são omissas quanto ao modo de execução de tais objetivos, nada dispondo, portanto, sobre o tratamento de dados pessoais que aquelas implicam (veja-se o caso do SAF-T ou, mais recentemente, do e-fatura).

Tal sucede aparentemente por opção político-legislativa, já que a CNPD, ao longo de vinte anos, nos seus pareceres sobre os referidos projetos de diploma legal – quando é consultada previamente –, tem sistematicamente chamado a atenção para esta omissão ou incompletude legislativa.

Ora, quando a lei é omissa quanto à regulação do tratamento de dados pessoais sensíveis, como é o caso, este carece de autorização da CNPD. Com efeito, os dados objeto de tratamento pela AT são dados sensíveis – nos termos definidos no n.º 1 do artigo 7.º da LPD – por corresponderem a informação relativa à vida privada dos cidadãos e por isso sujeita a um especial dever de sigilo. E, como decorre do artigo 28.º, n.ºs 1 e 2, se a lei não autoriza especificamente o tratamento de dados pessoais sensíveis e não define os diferentes aspetos deste, enunciados no n.º 1 do artigo 30.º da LPD, o tratamento depende de autorização prévia da CNPD.

Todavia, verifica-se que a AT ao longo dos anos tem vindo a criar novos tratamentos de dados pessoais sem prévia notificação à CNPD para efeito de emissão de eventual autorização. Situação, aproveita-se para notar, que se repete quanto a outros organismos da Administração Pública.

Ora, atenta a natureza sensível dos dados pessoais dos cidadãos que a AT trata, a regulação prévia dos tratamentos dos mesmos – *v.g.*, recolha, registo, conservação,

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

consulta, utilização, comunicação, interconexão, apagamento dos dados – é absolutamente necessária. Sobretudo, quando se considera a enorme quantidade e a diversidade de informação que a AT trata, informação que é disponibilizada pelos próprios cidadãos porque a isso estão obrigados nos termos da lei, ou que chega à AT, provindo de outras entidades públicas e privadas, por força de transmissões de dados, ora previstas em lei, ora produto de necessidades de ordem prática, relacionadas com a eficiência e simplificação administrativas.

Essa informação pessoal, importa sublinhar, abarca múltiplas vertentes da vida dos cidadãos, permitindo à Administração Pública, e a este organismo em especial, um conhecimento profundo da vida privada do cidadão, se a esse trabalho de análise individualizada e pormenorizada do "processo" de um cidadão a AT se dedicasse.

É por demais evidente que a dimensão dos tratamentos de dados pessoais aqui envolvidos afeta, restringindo seriamente, o conteúdo dos direitos fundamentais dos cidadãos: o direito à proteção de dados pessoais, previsto no artigo 35.º da CRP, o direito à reserva da intimidade da vida privada e familiar, previsto no n.º 1 do artigo 26.º da CRP, e ainda, na medida em que se difunda a perceção de que um nível mínimo de privacidade não está assegurado, o direito à liberdade, previsto no artigo 27.º, pelo evidente condicionamento da autonomia privada daí decorrente.

Cabendo estes direitos na categoria de direitos, liberdades e garantias, a regulação de tais restrições e a definição dos exatos termos em que os tratamentos podem ocorrer não pode senão ser feita por lei da Assembleia da República ou, observadas as orientações deste órgão de soberania quanto ao objeto e sentido da autorização legislativa, por decreto-lei autorizado – como determina o n.º 2 do artigo 18.º da CRP, mas resulta ainda da alínea b) do n.º 1 e do n.º 2 do artigo 165.º da CRP.

E o que se constata, também nesta área, é que, com exceção das normas contidas em lei do orçamento, a previsão de soluções fiscais que implicam o tratamento de dados pessoais vêm consagradas frequentemente em decretos-leis, em violação clara daqueles preceitos constitucionais.

Tudo isto se refere aqui para sublinhar que, se o legislador constituinte qualificou estes direitos como direitos, liberdades e garantias e reservou a definição dos termos e condições da sua restrição, condicionamento e promoção, à ponderação e decisão do principal órgão legislativo, a sistemática "delegação" da competência de definição do regime dos tratamentos de dados pessoais sensíveis, como os que aqui estão em causa, na Administração Pública parece estar longe de cumprir a prescrição constituinte.

Sobretudo, permite-se a CNPD notar, deve evitar-se, quando em causa está informação de natureza tão sensível, remeter a definição das garantias dos direitos dos cidadãos para a Administração Pública. Porque é isso que aqui está em causa. Quando se fala da definição dos termos e condições do tratamento de dados pensa-se na definição daquele perante quem o cidadão pode exercer os deus direitos fundamentais, designadamente, o direito de ser informado sobre as finalidades da recolha dos seus dados, o direito de aceder, conhecer, corrigir a informação ou pedir a sua eliminação. Mas também as condições em que o tratamento vai ocorrer, para que se definam claramente os limites do tratamento, os limites quanto à finalidade da utilização dos dados, quem pode aceder, em que condições e para que finalidade pode aceder, bem como as garantias de não discriminação do cidadão. Outros aspetos do regime poderão, deverão até, ser deixados para regulamentação administrativa; mas aqui, neste plano, apenas os aspetos práticos relacionados com a execução de tais garantias, que evidentemente não é tarefa do poder político-legislativo.

É bom de ver que não pode ser o responsável pelo tratamento de dados a definir os termos e condições fundamentais do tratamento de dados pessoais sensíveis, nem o seu superior hierárquico por via de regulamento administrativo.

Mesmo a delegação na CNPD da competência definidora dos termos e condições em que o tratamento de dados pessoais se faz, prevista no artigo 28.º da LPD (e no n.º 2 do artigo 7.º do mesmo diploma) – e que se justificará, em termos de opção legislativa, pela independência desta entidade e pela especialização dos seus conhecimentos – não deve ocorrer de modo regular e sistemático. Essa deve ser uma opção reservada para situações pontuais e menos estruturantes, em que ao legislador não seja possível prever, em abstrato, todos os aspetos essenciais do tratamento de dados pessoais – pela natureza recente e

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

inovadora de tecnologias possíveis naquele contexto ou pela elevada complexidade técnica do tratamento, por exemplo.

Nessa medida, a advertência que a CNPD por regra insere no final dos seus pareceres de que, caso o projeto de diploma legal em apreço não acautele todos os aspetos de regime, o tratamento está sujeito ao seu controlo prévio, não pretende mais do que chamar a atenção para essa fatalidade para que nos empurra o legislador nacional.

A primeira responsabilidade nas garantias dos direitos fundamentais dos cidadãos, quando em causa está informação pessoal dos cidadãos tratada pela AT, é, pois, do legislador, especificamente, da Assembleia da República.

Esta responsabilidade não afasta, é certo, a responsabilidade dos organismos da Administração Pública quando projetam e executam tratamentos de dados pessoais sem prévia autorização da CNPD para o efeito.

O facto de a CNPD reconhecer que boa parte dos tratamentos de dados pessoais realizados pela AT não está em conformidade com a lei, por não estarem regulados por lei, nem terem sido objeto de autorização prévia da CNPD, não tem levado àquela que seria a consequência lógica: proibir, temporária ou definitivamente, os tratamentos de dados pessoais (cf. alínea b) do n.º 3 do artigo 22.º da LPD).

Pelo contrário, o que a CNPD tem feito é, no âmbito da sua função de supervisão, na sequência das queixas de cidadãos ou da notícia de factos indiciadores de irregularidades nos tratamentos de dados pessoais, realizar inspeções e decidir em conformidade com o apurado: umas vezes, aplicando sanções, outras vezes, recomendando correções aos sistemas e aos procedimentos internos, para minimizar o impacto de tais tratamentos e práticas na privacidade dos cidadãos.

A razão de ser desta contenção interventiva prende-se com a consciência de que o princípio da legalidade, aqui diretamente invocável, não pode deixar de ser ponderado com outros valores constitucionalmente consagrados: o bloqueio da atividade da AT e de outros organismos públicos tem um tal impacto na vida dos cidadãos e na afirmação estrutural do Estado, que essa é uma medida administrativa de último grau, apenas aplicável quando o

conteúdo essencial dos direitos essenciais seja, de forma intensa e sistemática, afetado pela atividade daqueles organismos.

3.2 Política de segurança da AT

O documento que contém a política de segurança da AT nunca foi atualizado, contrariando o que nele vem prescrito quanto à necessidade da sua atualização periódica, nem mesmo quando a administração fiscal sofreu profunda reestruturação com a criação da AT e a integração de várias direções-gerais.

Acresce que não foram tomadas medidas organizacionais ou desenvolvidos procedimentos específicos com vista à implementação prática das políticas gizadas, em particular no que diz respeito ao cumprimento do regime de proteção de dados pessoais, tal como decorre dos artigos 14.º e 15.º da LPD.

Tal é revelador da importância diminuta atribuída à segurança da informação. Por outro lado, é notório que mesmo dirigentes de topo da AT, com responsabilidades na área dos sistemas de informação, desrespeitam de forma evidente a própria política de segurança, ao apagarem mensagens institucionais de correio eletrónico sobre assuntos relevantes e particularmente sensíveis, em espaço de dias, semanas ou meses, quando estão obrigados a guardar tais mensagens pelo período de cinco (5) anos.

Com efeito, é incompreensível e altamente censurável que as mensagens de correio eletrónico remetidas formalmente da ASI para a DSAI, para fins de auditoria interna, dando conta dos utilizadores/funcionários da AT que acederam a dados fiscais do Primeiro-Ministro e do Presidente da República, tenham sido apagadas pelo remetente, tal como a mensagem de resposta à DSAI sobre o universo da "lista VIP" e os critérios subjacentes à constituição desse grupo de contribuintes.

Além deste incumprimento, salienta-se a informalidade de procedimentos detetada, sendo alguns pedidos e respostas apenas tratados por telefone, donde não resulta qualquer registo

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

escrito e, consequentemente, a possibilidade de verificar a sua licitude. É este claramente o caso de um pedido dirigido à ASI para listar e identificar, por referência ao NIF do Primeiro-Ministro, todos os utilizadores que consultaram os seus dados fiscais numa determinada aplicação, relativa às execuções fiscais. Não é possível comprovar o contexto do pedido, logo aferir a legitimidade da recolha dessa informação, nem tão pouco controlar a sua utilização posterior.

Sem dúvida que a informalidade patente abre espaço à discricionariedade da administração, no plano procedimental. Todavia, a conformação discricionária dos procedimentos nesta matéria é sempre de evitar pelo risco que implica de diferenciação na tramitação dos processos.

Assume, por isso, especial gravidade o facto detetado pela CNPD de nem todos os acessos aos dados fiscais do Primeiro-Ministro e do Presidente da República terem sido reportados pela ASI à DSAI para o competente processo de auditoria, desconhecendo-se a razão por que tal não foi feito.

Em termos de política de segurança, é igualmente criticável o facto de haver apenas uma pessoa a desempenhar a tarefa de seriar os *logs* de acesso para a deteção de eventuais acessos abusivos, na medida em que essa pessoa não está sujeita a qualquer controlo.

Daqui resulta que não é verificável a licitude e a integridade dos dados recolhidos, designadamente se é retirada toda a informação disponível sobre quem acedeu ou se é feita qualquer seriação ou filtragem. Esta questão assume tanto mais relevância quanto do rol de funcionários identificados como tendo acedido a dados fiscais de contribuintes pode resultar na abertura de processos disciplinares ou participações criminais.

Ademais, omissões desta natureza fogem ao controlo do Conselho para a Prevenção da Corrupção, que funciona junto do Tribunal de Contas.

É pois essencial que haja um sistema de escrutínio, que permita garantir que a informação retirada é fiável e lícita, pelo que a tramitação procedimental em que a execução desta

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

função se traduz tem de estar taxativamente definida, não se compadecendo com informalidades nem tão-pouco com a centralização da tarefa numa única pessoa.

Ainda no quadro das políticas de segurança, verificou-se não estarem estabelecidos prazos mínimos de conservação de *logs*, sejam os que registam as operações realizadas pelos utilizadores da AT, sejam os que registam toda a atividade no Portal das Finanças, sejam ainda os relativos à própria gestão de utilizadores, isto é, os que permitem rastrear a atividade de quem cria, atribui e gere os perfis de acesso.

Os *logs* são conservados «enquanto houver espaço em disco». Tal foi a regra enunciada. Daqui se conclui não haver efetivamente uma orientação quanto a esta matéria. Se houver um aumento de atividade, como é normal, o prazo de conservação dos *logs* vai diminuindo, na proporção inversa. Sendo os prazos médios atuais bastante curtos (entre um e dois anos), em relação aos prazos de conservação da informação, a manter-se esta filosofia, pode chegar-se a prazos claramente ineficazes para os fins a que se destinam.

A exigência do registo de *logs* decorre do artigo 15.º da LPD, bem como das normas internacionais de segurança, para efeitos de controlo interno e para fins de auditoria externa, como aquelas realizadas pela CNPD.

A sua conservação deve, pois, verificar-se por prazo adequado à natureza do tratamento de dados em causa e deverá ter sempre uma duração mínima. Sempre se dirá a propósito que, apesar do grande volume de *logs* de que a AT reconhecidamente é geradora, hoje em dia os meios de armazenamento estão bastante melhorados e por muito menos custos.

Não há, pois, razão para que a AT não tenha uma rigorosa política de gestão e conservação de *logs*, no respeito pelas obrigações que decorrem dos artigos 14.º e 15.º da LPD.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

3.3 Gestão de acessos aos dados dos contribuintes

Da análise da política de gestão de acessos à informação fiscal dos contribuintes singulares, verifica-se haver um universo muito alargado de utilizadores a quem são atribuídos perfis de acesso bastante amplos, isto é, com a possibilidade de aceder a um vasto conjunto de informação.

Na verdade, mais de 75 por cento dos funcionários da AT têm privilégios para aceder à situação contributiva de qualquer cidadão e isto independentemente da sua localização geográfica ou das funções desempenhadas. Só em situações muito específicas, nomeadamente como as relacionadas com o e-fatura, há um maior controlo das permissões de acesso aos dados.

Apesar de existirem, na parte tributária, quatro grandes grupos de perfis, correspondendo às grandes divisões dos serviços (centrais, distritais, locais e lojas do cidadão), existe na prática uma enorme coincidência de permissões de acesso entre os grupos, donde decorre a possibilidade de aceder a um grande número de aplicações e, consequentemente, a várias categorias de dados pessoais, permitindo obter uma visão bastante global da situação de cada contribuinte.

Há ainda a considerar o acesso por parte de entidades externas à AT, tão variadas como sejam as empresas subcontratadas para o desenvolvimento e manutenção dos equipamentos e sistemas informáticos, os estagiários ou os tarefeiros contratados pelos serviços de finanças, num universo total superior a duas mil pessoas.

Analisando a lista de utilizadores externos, verifica-se haver um grande número de empresas privadas com permissão de acesso a dados contributivos, algumas das quais apresentam números francamente excessivos de utilizadores, das quais se destacam a Accenture com cerca de 120 utilizadores, a Novabase com cerca de 90 utilizadores e a Opensoft com mais de 60 utilizadores.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Esta realidade torna praticamente impossível um controlo efetivo por parte da AT da atividade levada a cabo por estes utilizadores, obrigação que detém à luz do artigo 14.º da LPD. Aqui se incluem, ademais, alguns utilizadores com perfis de administradores de base de dados (DBAs), fator que acentua a dificuldade de controlo de quem acede e/ou altera informação fiscal.

É notório não existir uma política de gestão de perfis de acesso que respeite o princípio da necessidade, assumindo-se genericamente que quase todos os utilizadores têm necessidade de aceder a quase tudo.

Por outro lado, estando essa tarefa atribuída a um grande número de responsáveis locais sem que haja critérios mais delimitadores na atribuição de perfis, bem como ferramentas tecnológicas que os imponham, é potenciado o número de utilizadores com a faculdade de aceder a informação de que, na realidade, não precisa para o desempenho das suas funções.

Deste modo, o risco de acesso abusivo aumenta substancialmente, tornando-se mais difícil controlar a atividade do universo de utilizadores. É, pois, manifesta a falta de ação preventiva por parte da AT, que salvaguarde a privacidade de cada um e de todos os cidadãos, quando está em causa informação particularmente sensível, principalmente pelo seu nível de agregação.

O princípio da necessidade não está, assim, ser cumprido, como exige a alínea c) do n.º 1 do artigo 5.º da LPD.

Mas também quanto a mecanismos reativos, apurou-se que a AT não realiza qualquer análise periódica de *logs* para detetar eventuais desvios nem realiza qualquer outro tipo de controlo regular (ou irregular) dos acessos efetuados. Limita-se a verificar *a posteriori* , na sequência de queixas ou de notícias publicadas, se houve acessos injustificados, e mesmo esse controlo verificou-se ser deficiente ao não incluir todas as aplicações.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Ora, esta situação não é de todo admissível, pois consubstancia uma demissão da AT das suas responsabilidades e obrigações legais, não acautelando devidamente a proteção dos dados pessoais dos contribuintes.

A opção de aceder ou não aos dados dos contribuintes não pode depender tão-só do juízo dos utilizadores, nem sobre eles recair em exclusivo a responsabilidade do acesso. Por mais sensibilização e formação que os funcionários possam ter – e nesse campo há quase tudo a fazer, pois só muito recentemente a AT começou a ministrar cursos sobre estas questões – é indispensável a adoção de sistemas de controlo efetivos que evitem acessos abusivos.

É, pois, ao responsável pelo tratamento de dados que incumbe zelar pela segurança do tratamento, designadamente proteger os dados pessoais de «qualquer forma de tratamento ilícito» (cf. n.º 1 do artigo 14.º da LPD).

3.4 Sistema de alarmística

Com base nos factos apurados, concluiu-se que foi levado à prática, durante cerca de quatro meses, um sistema de alarmística, baseado numa lista de contribuintes, donde resultou a comunicação formal de dois alertas para o serviço de auditoria para instrução dos respetivos processos.

Do conteúdo das comunicações trocadas entre a ASI e a DSAI, resulta claro que o sistema de alarmística esteve em efetiva produção, e que a realização de testes ocorreu «com sucesso» em momento anterior à apresentação da proposta, conforme resulta do ponto 10 da própria proposta.

Este sistema foi desenvolvido para confrontar todos os eventos (acessos, consulta e outras operações) com uma lista de NIFs pré-definida. Isto consubstancia um tratamento de dados pessoais, nos termos da alínea b) do artigo 3.º da LPD.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Todavia, à CNPD não foi submetida qualquer notificação deste tratamento de dados pessoais, como é exigência do n.º 1 do artigo 27.º da LPD.

Como foi atrás referido, a AT não tem mecanismos adequados e eficazes de controlo dos acessos aos dados pessoais dos contribuintes, não adotando uma atuação preventiva e, mesmo reativamente, só age em determinadas circunstâncias.

Assim sendo, num contexto de deficiente proteção dos dados pessoais dos contribuintes, não se compreende a adoção de um sistema exclusivo para controlo dos acessos a um grupo específico de contribuintes. Tal ação é geradora de discriminação ao nível das garantias oferecidas, sem que seja em si mesma impeditiva de eventuais acessos abusivos. Na verdade, tal prática origina uma diferenciação de tratamento dos cidadãos, na medida em que implica uma ação sancionatória célere somente para certos casos, o que pode ter um efeito dissuasor do acesso aos dados de apenas alguns contribuintes, logo não garantindo a mesma proteção para todos.

O valor acrescentado que eventualmente poderia resultar deste sistema – se funcionasse em tempo real – seria uma contenção de danos ao evitar a propagação pública da informação. Na prática, nada no desenho deste sistema de alarmística preveniria a possibilidade de acesso abusivo.

Tal só poderá ser alcançado com outro tipo de medidas, como acima mencionado. Se a AT aplicar políticas gerais de segurança e de gestão de perfis adequadas, recorrendo designadamente a soluções tecnológicas aptas, assegurará um nível elevado de proteção da informação para todos os contribuintes, o que naturalmente também protegerá aqueles que possam estar, por motivos variados, mais expostos à curiosidade alheia.

4. Conclusões

A inspeção levada a cabo pela CNPD permitiu confirmar a existência de um conjunto de acessos claramente excessivo e indiciador de ilicitude. Todavia, tendo-se verificado que os

procedimentos e práticas institucionalizados na AT não só não promovem como facilitam o acesso indiscriminado aos dados dos contribuintes, entende a CNPD que o juízo de censura último não pode deixar de recair sobre a AT.

Da análise atrás realizada, decorre a necessidade de serem estabelecidas regras inequívocas sobre os tratamentos de dados da responsabilidade da AT e medidas que efetivamente assegurem a proteção dos dados pessoais dos cidadãos.

Assim, a CNPD vem, no exercício das competências definidas no n.º 4 do artigo 22.º e no n.º 4 do artigo 23.º da Lei n.º 67/98, de 26 de outubro, sugerir à Assembleia da República a aprovação de diploma legal que regule o conjunto dos tratamentos de dados pessoais efetuados pela AT.

A CNPD vem ainda determinar que sejam adotadas soluções técnicas e organizacionais idóneas a tutelar os direitos fundamentais de todos os contribuintes.

Para o efeito, considera ser indispensável:

4.1 Na execução da adoção de medidas preventivas de acessos abusivos, a definição rigorosa de uma política de gestão de perfis de acesso, que tenha como princípio norteador a adequação, a necessidade e a proporcionalidade, bem como de mecanismos eficazes de controlo de acessos aos dados fiscais de todos os cidadãos;

4.2 Que os acessos sejam contextualizados, isto é, relacionados sempre com um evento (atendimento do contribuinte, tramitação de um processo específico, pedido formal de informação, etc.);

4.3 Adicionalmente, que sejam encontradas soluções tecnológicas que, em determinadas circunstâncias, não impedindo em absoluto o acesso, obriguem o utilizador a reequacionar a sua necessidade;

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

4.4 Dar especial atenção aos perfis de acesso para utilizadores externos, os quais devem ter credenciais atribuídas por períodos de tempo limitados e estritamente adstritos às funções a desempenhar;

4.5 Estabelecer prazos fixos de manutenção dos *logs*, atendendo à natureza dos dados a proteger e ao período de conservação dos dados;

4.6 Definir padrões de utilização de acesso à informação que permitam aferir comportamentos anómalos, de forma automatizada, quando for efetuada a análise periódica dos *logs*;

4.7 Definir regras claras para a tramitação do procedimento de controlo dos acessos, erradicando as práticas informais e garantindo um sistema eficaz não assente no desempenho desta função por um só funcionário;

4.8 Que, neste âmbito, os pedidos de consulta da DSAI e as respostas da ASI devam ser realizados num sistema próprio, auditável, que garanta confidencialidade, integridade e não repúdio, sob pena de não servirem como documento com valor probatório; de facto, um simples *e-mail* não reúne nenhum daqueles requisitos;

4.9 Que a AT continue a desenvolver ações de formação para os dirigentes e funcionários, com especial ênfase na proteção de dados pessoais;

4.10 Por último, atenta a dimensão e dispersão territorial da administração fiscal, bem como a sensibilidade dos dados pessoais tratados, sugere-se a designação de um Delegado de Proteção de Dados, que tenha por função garantir o cumprimento pela AT do regime de proteção de dados pessoais, antecipando o novo quadro legal europeu nesta matéria.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Notifique-se o responsável pelo tratamento de dados da AT, na pessoa do Diretor-Geral da Autoridade Tributária e Aduaneira, do teor desta deliberação, fixando-se o prazo de seis meses para que a AT comunique à CNPD quais as medidas técnicas e organizacionais que vai adotar para dar cumprimento às determinações supra elencadas.

Nos termos do disposto no n.º 5 do artigo 22.º da LPD, cumpre denunciar ao Ministério Público as infrações penais de que a CNPD tenha conhecimento, no exercício das suas funções e por causa delas. Deste modo, tendo sido recolhidas provas que podem indiciar ilícitos criminais, a CNPD determina a extração de certidões de todo o processado a remeter ao Ministério Público.

Dê-se conhecimento da presente deliberação à Comissão de Orçamento, Finanças e Administração Pública da Assembleia da República e ao Secretário de Estado dos Assuntos Fiscais.

Os documentos anexos ao Relatório de Inspeção não são tornados públicos, por conterem informação que deve ser protegida por questões de segurança.

Lisboa, 31 de março de 2015

Filipa Calvão (Presidente)

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Relatório de Inspeção

No dia 16 de março de 2015, uma equipa de técnicos da CNPD, constituída por Isabel Cristina Cruz, Vítor Bernardo, Clara Guerra e Marta Jacinto, deslocou-se às instalações da Autoridade Tributária e Aduaneira (AT), sitas em Lisboa, na Av. Eng.º Duarte Pacheco, 28 (edifício Satélite) e na Rua da Prata, n.º 10, para realizar ação inspetiva conforme despacho da Presidente da CNPD, da mesma data.

No dia 19 de março de 2015, os técnicos da CNPD Isabel Cristina Cruz, Vitor Bernardo e Clara Guerra deslocaram-se às instalações da AT, sitas em Lisboa, na Rua da Alfândega, n.º 5, e na Av. Eng.º Duarte Pacheco, 28 (edifício Satélite) para continuação da ação de fiscalização.

A presente inspeção contou com a realização de verificações nos sistemas de informação e com a recolha de testemunhos de dirigentes e funcionários da AT, bem como do Presidente do Sindicato dos Trabalhadores dos Impostos, identificados no decurso do relatório. Procedeu-se também à recolha de documentação.

*

No dia 16 de março de 2015, foi contactado telefonicamente o Presidente do Sindicato dos Trabalhadores dos Impostos, Paulo Ralha, sobre a informação de que poderia dispor, face às declarações públicas por si prestadas. Das suas afirmações não resultou qualquer informação adicional em relação ao já anteriormente publicado pela comunicação social.

Das diligências efetuadas, apuraram-se as informações abaixo descritas.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

1. Acesso aos sistemas de informação da AT

Sobre a forma como é realizado e gerido o acesso aos sistemas de informação da AT, bem como as medidas de segurança aplicadas, prestaram declarações a Engª Graciosa Martins Delgado (GMD), coordenadora da Área de Gestão de Impostos, que afirmou estar a desempenhar funções de Subdiretora Geral de Sistemas de Informação (SDGSI), o Dr. José Morujão Oliveira (JMO), a chefiar a Área de Segurança Informática (ASI) e a Dra. Ângela Santos, diretora da Direção de Serviços de Gestão de Recursos Humanos (DSGRH).

1.1 Atribuição e gestão de acessos dos funcionários

A gestão de utilizadores dos sistemas de informação da AT é feita numa aplicação específica denominada Sistema de Gestão de Utilizadores (SGU). Em cada serviço, há um responsável local (poderá haver mais se o universo de utilizadores em causa for muito grande), designado pela respetiva chefia, ou ser o próprio chefe, que está incumbido da gestão de utilizadores somente desse serviço. Essa pessoa tem poderes para criar, alterar ou eliminar utilizadores e para atribuir os perfis de acesso, que tem disponíveis conforme a sua "área de negócio". Na área tributária, estão definidos quatro grandes grupos de perfis, de acordo com as competências dos serviços envolvidos: serviços centrais, serviços de finanças (repartições), direções de finanças (distritais) e lojas de cidadão. Encontra-se assim estabelecido para cada um destes grupos de perfis quais os sistemas de informação (aplicações) passíveis de serem acedidos (DOC1).

Verifica-se que o número de aplicações acessíveis em cada um destes grupos de perfis é bastante extenso e, em grande parte, coincidente, donde resulta que é possível conhecer a situação contributiva de qualquer cidadão, independentemente do grupo em que o utilizador se insere.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Foi declarado que, num universo de 12.156[1] de utilizadores internos, existe um total de 9.298 funcionários com este tipo de permissão de acesso (direções de finanças: 1.935; serviços centrais: 1.834; serviços de finanças: 4.515; serviços aduaneiros: 1.014). Há ainda a considerar 2.302 utilizadores externos[2] com os mesmos níveis de permissão (DOC2).

1.2 Interação com outros organismos públicos

A AT interage com outros organismos públicos a diferentes níveis[3]. Conforme declarações prestadas sobre esta matéria, há entidades públicas com acesso autorizado para carregar informação no Portal das Finanças no âmbito dos pedidos de penhora para execução pela AT; há entidades que protocolaram com a AT que a autenticação de cidadãos nos seus sítios da Internet seja feita com a credenciação que os contribuintes detêm na AT (são disso exemplo, nomeadamente, o Instituto de Mobilidade e dos Transportes ou o Banco de Portugal); há ainda o caso da Segurança Social (SS) que troca um vasto conjunto de informação com a AT (DOC5).

Sobre a cooperação entre a Segurança Social e a AT, prestou ainda declarações a Dra. Matilde Lopes.

---

[1] Verificou-se que este número não esgota a totalidade dos utilizadores com acesso a esta informação, não sendo possível determinar com rigor o universo total de utilizadores.

[2] No conceito de utilizadores externos, integram-se, de acordo com o declarado, tarefeiros nos serviços de finanças, estagiários, equipas de desenvolvimento e manutenção em regime de subcontratação, DBAs e, ainda, funcionários da AT a prestar serviço num segundo local.

[3] A Engª Graciosa Martins Delgado comprometeu-se a remeter à CNPD a lista dos protocolos celebrados entre a AT e outras entidades com um sumário do seu objeto. Até à data do presente relatório, não foi recebida a informação solicitada.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Do conjunto das declarações prestadas resultou haver três tipos de fluxos de dados entre a AT e a SS:

- O envio do *Anexo SS*, submetido pelo contribuinte à AT e reencaminhado por *webservice* para a Segurança Social;
- Consulta por *webservice*, em sistema de *hit/no hit*, por um lado, por parte da AT à SS sobre eventuais dívidas à segurança social para fins de atribuição de benefícios fiscais e, em sentido inverso, por parte da SS à AT sobre a existência de eventuais dívidas fiscais para fins de atribuição de benefícios sociais.
- Transmissão recíproca de dados entre a AT e a Segurança Social, através de acesso FTP, conforme definido em Protocolo de Cooperação e Coordenação de Procedimentos entre os Serviços da Administração Fiscal e das Instituições da Segurança Social[4]. De acordo com as informações prestadas, esses fluxos de dados realizam-se com periodicidade mensal.

Questionados especificamente sobre a eventual existência de utilizadores da Segurança Social credenciados para aceder e consultar diretamente a informação contida nas aplicações da AT, foi claramente declarado por GMD e por JMO não existirem tais privilégios de acesso.

Declararam ambos não haver qualquer entidade com esses privilégios de acesso direto, não existindo utilizadores credenciados para esse fim, mas apenas as modalidades de acesso acima descritas. Estas afirmações não foram verificadas pela equipa de inspeção.

[4] Protocolo homologado em 6 de dezembro de 2004 pelo Ministro das Finanças e da Administração Pública e pelo Ministro da Segurança Social, da Família e da Criança.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2. Política de segurança da AT

Existe um documento, designado por Política de Segurança da Informação da Administração Fiscal e Aduaneira, com a referência *Proc.: AT.99.01.00.01*[5], no qual é expresso o objetivo de *estabelecer os princípios orientadores da composição dum sistema que responda às solicitações da administração fiscal e aduaneira em matéria de protecção da informação processada por computador e assegure a continuidade das operações, minimizando o impacto de incidentes de segurança* (DOC3).

Existe também um documento denominado Carta de Princípios, que descreve a *filosofia inerente à segurança da informação na administração fiscal e aduaneira, identifica o escopo da segurança, descreve os respectivos princípios, define o âmbito das políticas e atribui responsabilidades* (DOC4).

No que respeita ao procedimento de atribuição de credenciais de acesso, o código do utilizador (*userID)* é composto pela primeira letra do primeiro e último nome, seguido do número mecanográfico do funcionário, e a palavra-passe é gerada aleatoriamente e remetida por carta ao funcionário, que a deve alterar na primeira utilização.

Existem regras escritas para a composição da *password* na política de segurança da AT.

A conta de utilizador é bloqueada automaticamente após 90 dias de inatividade. Para que volte a poder ser usada é necessário reativar o utilizador. Mensalmente, os recursos humanos remetem à ASI uma lista de funcionários aposentados, procedendo a ASI diretamente à eliminação desses utilizadores.

Existe um histórico da gestão de utilizadores, guardado «aproximadamente pelo período de 3 anos, enquanto houver espaço em disco». Os *logs* de criação e gestão de utilizadores são guardados por um ano.

[5] O documento disponibilizado a pedido da equipa não tem data e indica ser a versão 1, tendo sido declarado que era a única versão existente.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

As operações realizadas nas aplicações da AT pelos funcionários, designadamente o acesso, a alteração, a impressão, são igualmente registadas em *logs*. Estes não estão uniformizados entre aplicações, mas tipicamente registam *userID*, aplicação utilizada, NIF consultado, tipo de operação, data e hora e mensagem de ok/erro sistema.

Os *logs* são agregados (com exceção das aplicações ainda em *Mainframe*) e indexados recorrendo ao *software Splunk*, e servem os propósitos de segurança/alarmística (relatório de ataques a *firewall*, ocupação de disco, etc.), auditoria e apoio aos contribuintes na resolução de problemas de acesso. Nesta ferramenta estão configuradas notificações automáticas associadas ao desempenho dos sistemas e a situações de risco de segurança. Além disso, o *Splunk* permite a consulta de estatísticas, designadamente sobre taxas de utilização (por exemplo, maior número de pesquisas num determinado intervalo de tempo) que poderá permitir, após análise, detetar um comportamento de desvio.

Foi declarado que os *logs* de acesso e outras operações realizadas pelos utilizadores nas aplicações são guardados, dependendo do espaço em disco, por um período «entre um e dois anos» e afirmado que não é realizada uma análise periódica e regular desses registos.

Não são registados os IPs das máquinas internas. Só no Portal das Finanças, são registados os IPs de origem, bem como todo o circuito de navegação e operações efetuadas pelos contribuintes, técnicos oficiais de contas (TOC) e outras entidades com acesso ao Portal.

Foi ainda declarado que não estão configurados alertas no sistema para deteção de potenciais acessos indevidos/abusivos.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

3. Processos de auditoria por eventual acesso abusivo a dados de contribuintes

3.1 Descrição dos procedimentos

Sobre os processos de auditoria abertos por acessos eventualmente abusivos a dados de contribuintes, o circuito da informação e os procedimentos estabelecidos na AT neste contexto, prestaram esclarecimentos o Dr. Serafim Pereira (SP), Diretor da Direção de Serviços de Consultadoria Jurídica e Contencioso (DSCJC), GMD, JMO, Acácio Pinto (AP), Diretor da Direção de Auditoria Interna (DSAI) e Vítor Lourenço (VL), chefe da Divisão de Acompanhamento dos Resultados de Auditorias, Planeamento e Apoio Técnico (DARPAT), o qual foi ouvido nas instalações da CNPD, no dia 19 de março.

Os processos de auditoria por eventuais acessos abusivos são desencadeados a partir de denúncias, queixas ou notícias na comunicação social. Relativamente a estas últimas, o representante da DARPAT informou que existe um serviço de revista de imprensa, cuja análise permite detetar e atuar quando há notícias que indiciem violações nas matérias da sua competência.

Nesse caso, o técnico auditor faz uma análise preliminar, propõe a abertura de processo de auditoria ao diretor da DSAI, que se anuir, remete para o Diretor-Geral que, por sua vez, determina ou não a abertura de processo. Sendo determinada a abertura de processo são solicitados, por *e-mail*, à ASI, informação sobre os eventuais acessos aos dados de um contribuinte identificado ou informação dos acessos realizados por um determinado funcionário, num intervalo de tempo específico.

JMO confirmou que a deteção de acessos eventualmente abusivos era apenas possível através de pesquisa desencadeada de forma manual no sistema *Splunk*, o que só acontecia no seguimento de pedidos remetidos, por *e-mail* ou por ofício, à ASI ou diretamente a ele próprio, provenientes, por regra, do Ministério Público ou da DSAI. Os técnicos da CNPD verificaram alguns desses pedidos.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

JMO informou que, para responder a cada pedido, efetua uma pesquisa no sistema *Splunk* pelo NIF ou nome de utilizador dentro de um determinado intervalo de tempo indicado no pedido, exporta os resultados da pesquisa, identifica os utilizadores ou lista os contribuintes consultados e remete esta informação para o organismo requerente.

Retomando os trâmites do processo de auditoria, VL afirmou que, obtida a resposta da ASI, o auditor faz a instrução do processo, procedendo à audição dos utilizadores identificados na resposta, no sentido de apurar a legitimidade dos acessos. Encerrada a instrução, é efetuado um relatório a homologar pelo Diretor-Geral que contém recomendações.

Se o relatório concluir pela eventual violação de deveres funcionais, será remetido para a DSCJC. Todos os relatórios de auditoria são enviados para o Conselho para a Prevenção da Corrupção, que funciona junto do Tribunal de Contas.

3.2 Os casos concretos

Para confirmação do procedimento descrito para a pesquisa de acessos no sistema *Splunk*, foi determinada uma busca nos *logs* de acesso com os seguintes parâmetros: período entre 16/3/2014 e 16/3/2015 para os NIFs dos contribuintes Pedro Manuel Mamede Passos Coelho (NIF:177142430) e Aníbal António Cavaco Silva (NIF:125507410) (DOC6). O resultado desta pesquisa[6] indicou 137 acessos aos dados fiscais do Primeiro-Ministro, efetuados por 41 utilizadores distintos, e 9 acessos aos

[6] O sistema *Splunk* agrega os *logs* de pesquisas, consultas e modificações produzidos pelas aplicações da AT. Isto significa que uma operação de alteração pode ter múltiplos registos associados (atendendo a que uma modificação terá subjacentes uma pesquisa e uma consulta). Assim, o volume de resultados deve ser analisado atendendo à data do acesso e ao utilizador em questão.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

dados fiscais do Presidente da República, efetuados por 4 utilizadores. Estas pesquisas foram apenas relativas à aplicação de IRS.

Foi também efetuada uma busca nos *logs* de acesso com o NIF de um dos técnicos da equipa da CNPD, não apenas quanto ao IRS, mas relativa a todas as aplicações, para o período entre 1/1/2015 e 16/3/2015. O retorno permitiu concluir que não existiam *logs* de acessos à aplicação de IRS, mas apenas *logs* de acesso do próprio ao e-Fatura no *Portal das Finanças.*

Quanto a casos concretos, VL declarou que, em 2013, foi aberto processo de auditoria com base em notícia publicada na imprensa, relativa a informação fiscal do ex-Ministro da Economia, Manuel Pinho. Disse que, em meados de 2014, foi aberto outro processo também na sequência de notícia publicada que indiciava o acesso a informação fiscal da mãe do ex-Primeiro-Ministro José Sócrates.

Declarou, também, que no dia 26 de setembro de 2014, foi aberto processo de auditoria decorrente da publicação de uma notícia no jornal i, indiciadora de acesso abusivo a dados fiscais do Primeiro-Ministro, Pedro Passos Coelho.

SP da DSCJC confirmou que no «final de dezembro, início de janeiro» receberam o relatório de auditoria da DSAI, do qual resultaram 27 processos disciplinares, que estarão em fase final de tramitação. Este dirigente referiu que existem «outros processos da mesma natureza relativamente a outras figuras públicas».

VL afirmou que estes casos, em particular a justificação dos funcionários de que acederam «*por mera curiosidade*», criaram na DSAI a convicção da necessidade de dar formação específica aos funcionários e dirigentes da AT. Esta convicção foi reforçada com as notícias que indiciaram o acesso aos dados fiscais do Primeiro-Ministro, uma vez que na instrução do processo se concluiu terem existido cerca de 30 funcionários que acederam à informação, os quais, na sua grande maioria, apresentaram essa mesma justificação. Afirmou ainda haver a convicção que a mera

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

consulta, sem divulgação da situação tributária, não configurava ilícito disciplinar ou criminal.

4. Formação de funcionários e dirigentes da AT

Acerca da formação de funcionários e dirigentes, informou o Chefe de Divisão da DARPAT, que, em 2014, foi criado um grupo de trabalho transversal, envolvendo a área de auditoria, a área de disciplina e a área da segurança informática, para desenvolver um plano de formação para a sensibilização dos funcionários e dirigentes da AT. Nessa sequência, foi organizado um curso «Normas de conduta e política da segurança da informação», constituído por quatro módulos: organização na AT; ética no trabalho e risco de corrupção, segurança informática e exercício do poder disciplinar.

Neste âmbito, foram organizadas duas sessões de formação em Lisboa e uma no Porto, dirigidas a mil novos inspetores tributários. Foram também desenvolvidos conteúdos para formação em *e-learning*, a qual acompanha um conjunto de sessões distritais presenciais para dirigentes.

5. Sistema de "alarmística" – "Lista VIP"

Aquando da primeira ação fiscalizadora à AT, no dia 16 de março de 2015, JMO afirmou nunca ter recebido «qualquer lista de contribuintes, por meio algum, de qualquer proveniência». Referiu ainda não estarem implementados alertas automáticos associados aos acessos efetuados pelos utilizadores. Também GMD declarou, na mesma altura, não haver alertas associados a consultas aos dados de contribuintes.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Perguntado especificamente sobre se tinha conhecimento da existência de um qualquer sistema de alerta ou notificação em caso de acesso aos dados pessoais de determinados contribuintes, JMO asseverou não existir tal mecanismo ou lista VIP associada.

Atendendo às afirmações que terão sido efetuadas por VL numa ação de formação para inspetores tributários, que decorreu em 20 janeiro de 2015, em Lisboa, sobre a existência de um sistema de alerta de acessos associado a um «pacote VIP» de contribuintes, convocou-se VL para prestar declarações, o que veio a acontecer no dia 19 de março de 2015, nas instalações da CNPD.

Questionado sobre a justificação para as suas declarações na ação de formação de janeiro, respondeu estar convicto da existência de tal sistema de alerta, tendo, no essencial, afirmado o seguinte: a existência de um despacho, de 10 de outubro de 2014, do Subdiretor-Geral José Maria Pires, agindo na qualidade de substituto legal do Diretor-Geral da AT, a determinar a criação de um sistema de alarmística, associado a uma lista VIP, bem como o recebimento na DSAI de dois alertas com origem neste sistema.

Disse também que a sua convicção foi posteriormente reforçada, quando a ASI, em 24 de fevereiro de 2015, remete à DSAI a lista dos contribuintes.

Face a estas declarações, entendeu-se ser essencial recolher a prova documental na DSAI, o que se fez no mesmo dia, conforme autos de apreensão juntos (DOCs 8 e 9).

Com base na análise dos documentos e informações recolhidos, apurou-se o seguinte:

- Em 3 de outubro de 2014, foi remetida pela ASI ao Gabinete da SDGSI, a Informação ASI/238/2014, datada de 30 de setembro de 2014 e assinada por JMO, referente a "Controlo do Acesso aos Dados – alarmística em caso de consulta/alteração de dados sensíveis" (DOC 8b).

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

- Esta Informação consiste numa proposta para a configuração de alertas que seriam *despoletados em caso de verificação de consulta ou alteração de dados de determinados contribuintes que, na ausência de melhor conceito, denominamos VIP*. A proposta referia, no ponto 6 alínea b) que os alertas seriam remetidos por correio eletrónico da ASI para a DSAI para avaliação da legitimidade do acesso, e na alínea c) do mesmo ponto, que, *na sequência do resultado da avaliação, a DSAI propõe ao senhor Diretor-Geral da AT as ações que considerar adequadas*.

- No ponto 9 da proposta é referido *que [p]ara implementação deste procedimento é requisito indispensável a identificação dos NIFs que ficarão sobre monitorização, sugerindo-se que, numa fase inicial, se incluam, pelo menos, os principais titulares dos órgãos de soberania*. Por fim, a proposta referia no ponto 10 que [*a*] *solução tecnológica foi testada com sucesso*.

- No dia 9 de outubro, o GSDG dos Sistemas de Informação remete a Proposta da ASI para o Gabinete do Diretor-Geral, com o parecer favorável de GMD, com o seguinte teor:

> «*Concordo com o proposto.*
> *A atribuição de perfis para acesso aos dados é feita pelas chefias através da aplicação de Gestão de utilizadores.*
> *O sistema de alertas, aqui proposto, permite detectar acessos potencialmente indevidos e assim prevenir situações de divulgação de notícias lesivas para a imagem da AT.*
> *À consideração superior*
> *Graciosa Delgado*»

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt
21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- No dia 10 de outubro de 2014, o Subdiretor-Geral de Justiça Tributária, Dr. José Maria Pires (JMP), apõe despacho com o seguinte teor:

> *«Concordo. Proceda-se como vem proposto.*
> *A DSAI apresentará relatório da avaliação da medida até ao final do ano corrente, bem como proposta de implementação de uma medida definitiva de salvaguarda do sigilo contra usos abusivos ou indevidos, incluindo o âmbito de abrangência da presente proposta.*
> *2014-10-10*
>
> *Assinatura ilegível*
> *SUBSTITUTO LEGAL*
> *DO DIRETOR-GERAL*
> *José Maria Pires*
> *Subdiretor-Geral»*

- No dia 13 de outubro de 2014, o despacho é remetido ao Gabinete de GMD, que o recebe a 15 de outubro de 2014 e o remete a JMO, autor da Informação.

- No registo de correspondência, este documento recebeu o n.º 2014022511.

- Em 20 de outubro de 2014, JMO enviou, por *e-mail*, para o Dr. Acácio Pinto (AP) a Informação ASI/238/2014, com o parecer de GMD e o despacho favorável do Subdiretor-Geral (DOC 8a).

- Em 24 de outubro de 2014, o Diretor da DSAI, pediu esclarecimentos relativamente à dita proposta, quanto à sua concretização, designadamente sobre o conteúdo e periodicidade dos alertas previstos, bem como a forma pela

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

qual eles chegariam à DSAI e a partir de que data a remessa de alertas através de correio eletrónico se iniciaria (DOC 8c).

- Ainda no dia 24 de outubro de 2014, respondeu JMO, clarificando que os alertas seriam enviados para a ASI, onde seriam tratados antes de serem remetidos para a DSAI, e que *o início do processo está apenas dependente da indicação à ASI dos NIFs que serão objeto de alerta*, salientando que *[q]uando refiro ASI quero dizer apenas os funcionários que têm como tarefa obter este tipo de informação (neste momento sou apenas eu)* (IDEM).

- No dia 24 de outubro de 2014, AP emite Ordem de Serviço a abrir processo de auditoria- a DSAI abriu um processo geral para a alarmística com a referência 457/DARPAT/2014 (DOC 9c);

- No dia 6 de novembro de 2014, às 17:18, JMO remeteu ao Diretor da DSAI um *e-mail* a comunicar o *resultado dos alertas de segurança que temos implementados para as operações de consulta/alterações relativamente ao NIF 177142430* (NIF do Primeiro-Ministro, Pedro Passos Coelho). Neste *e-mail* está identificada uma consulta efetuada pelas 15:51 desse dia, discriminando o nome do funcionário e da repartição de finanças a que pertence. Este *e-mail* foi em cópia para GMD (DOC 8d).

- No dia 28 de novembro de 2014, às 12:31, JMO remeteu ao Diretor da DSAI um *e-mail* a comunicar o *resultado dos alertas de segurança que temos implementados para as operações de consulta/alterações relativamente ao NIF 125507410* (NIF do Presidente da República, Aníbal Cavaco Silva). Neste *e-mail* está identificada uma consulta efetuada pelas 12:34 do dia 24 de novembro de 2014, discriminando o nome do funcionário e da repartição de finanças a que pertence. Este *e-mail* foi em cópia para GMD (DOC 8e).

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- Foi declarado por AP que estas duas comunicações foram juntas ao processo de auditoria relativo à alarmística, com o n.º 457/DARPAT/2014 e foram objeto de instrução.

- Foi declarado por AP e VL que no dia 18 de fevereiro de 2015, a DSAI solicitou à ASI a informação sobre *quais os critérios subjacentes à constituição do grupo de contribuintes a monitorizar, denominados de "VIP", assim como a sua identificação (NIF e nome).* Solicitou também informação sobre *se o respectivo universo se manteve estável ou se foi objecto de alterações e, em caso afirmativo, qual a data em que ocorreram essas alterações e identificação dos contribuintes do universo (NIF e nome) em cada um desses momentos.*

- No dia 23 de fevereiro de 2015, o Diretor-Geral da AT, António Brigas Afonso, sobre a Informação ASI/238/2014, emite despacho com o seguinte teor:

> *«E.T. Fica sem efeito o presente procedimento*
> *C/C à DSAI*
> *Em 2015/02/23*
> *Assinatura ilegível*
> *António Brigas Afonso*
> *Diretor-Geral»*

- No dia 24 de fevereiro de 2015, pelas 11:40, a DSAI envia um *e-mail* à ASI, insistindo na obtenção de resposta ao seu pedido de 18 de fevereiro (DOC 11).

- No dia 24 de fevereiro de 2015, pelas 12:04, a ASI respondeu por *e-mail*, informando com cópia para a GMD, acerca do *universo sujeito a alerta VIP"* (DOC 9b), a saber:

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

RE: Informação nº ASI-238/2014
ASI - Área de Segurança Informática
Enviado: terça-feira, 24 de Fevereiro de 2015 12:04
Para: DSAI - DARPAT - Planeamento
Cc: Graciosa Martins Delgado

Bom dia.

Conforme solicitado informo que o universo sujeito a alerta "VIP"é o seguinte:

Passos Coelho NIF 177142430
Cavaco Silva: NIF 125507410
Paulo Portas: NIF 132239264
Paulo Núncio: NIF 181982730.

Os 3 primeiros NIFs foram obtidos de pesquisa na Internet e foram inseridos de início. O último NIF foi inserido na sequência do processo de auditoria sobre consultas efetuadas aos dados fiscais do senhor SEAF.

Tal como referido no ponto 9 da informação ASI-238/2014, aguardo indicação sobre qual o universo a abranger.

Cumprimentos,

ASI - Área de Segurança Informática
Av. Eng. Duarte Pacheco, nº 28 - 8º - 1099-013 Lisboa
Geral: (+351) 213 834 200 - Fax: (+351) 213 834 974
CAT - Centro de atendimento telefónico - (+351) 707 206 707
E-mail: asi@at.gov.pt Visite-nos em www.portaldasfinancas.gov.pt

- No dia 2 de março de 2015, a DSAI recebe o despacho do Diretor-Geral, de 23 de fevereiro, revogando o despacho que instituiu o procedimento de alarmística (DOC 9d).

Questionado o Diretor da DSAI sobre a existência do processo de auditoria a eventuais acessos indevidos aos dados fiscais do Secretário de Estado dos Assuntos Fiscais (SEAF), Paulo Núncio, referido na resposta da ASI de 24 de fevereiro, declarou nunca ter existido qualquer processo de auditoria interna relacionado com o SEAF.

Da análise dos elementos recolhidos, constatou-se terem havido contradições e incongruências significativas, entre as provas documentais obtidas e as declarações de JMO e GMD, prestadas no dia 16 de março de 2015, pelo que, no dia 19 de março de 2015, a equipa de inspeção realizou diligências adicionais, junto daqueles dois dirigentes.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

Pesquisando as comunicações institucionais relativas ao envio dos alertas nos dias 6 e 28 de novembro, quer na conta ASI, quer na conta de JMO, bem como a informação prestada a 24 de fevereiro de 2015 sobre a lista de VIPs, todas elas remetidas à DSAI, não foi encontrada nenhuma destas mensagens, o que constitui um forte indício de que as mensagens foram apagadas da caixa de correio do diretor da ASI.

No servidor de *e-mail* (*Microsoft Exchange*), que apenas conserva os *logs* pelo período de três meses, obtiveram-se ainda os *logs* do *e-mail* recebido pela ASI às 11:40, de 24 de fevereiro de 2015, e do *e-mail* de resposta remetido à DSAI pelas 12:04 do mesmo dia (DOC 12).

Questionado de novo sobre a existência de alguma iniciativa interna, com vista ao controlo de acessos indevidos a dados dos contribuintes, JMO admitiu ter feito uma proposta «para implementação de um mecanismo automático de alarmística, baseado no software *Splunk*, que foi aprovada pela Engª Graciosa Delgado e pelo então substituto legal do Diretor-Geral, Dr. José Maria Pires».

Sobre que medidas tomou para a implementação do procedimento, declarou que não tinha feito nada, «porque a DSAI tinha que entregar uma lista». Confrontado com o despacho do Subdiretor-Geral *«Concordo. Proceda-se como proposto»,* JMO continuou a declarar não ter tomado qualquer medida, porquanto teria entendido do despacho que a DSAI lhe enviaria uma lista.

Insistindo-se que dificilmente se poderia retirar do despacho tal interpretação, uma vez que à DSAI competiria, antes de mais, fazer um relatório de avaliação da aplicação do procedimento alarmístico, JMO acaba por admitir que o sistema funcionou em testes. No entanto, não foi capaz de precisar a duração dos supostos testes, o seu início ou fim. Disse não se recordar e não ter disso registo.

O JMO informou que, previamente à apresentação da proposta e de forma a testar o mecanismo de alarmística que iria propor, configurou o sistema *Splunk* para produzir alertas perante eventos de consultas a determinados contribuintes.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

Para isso, coligiu, por sua iniciativa, os números de contribuinte do Primeiro-Ministro (Pedro Passos Coelho), do Vice-Primeiro-Ministro (Paulo Portas) e do Presidente da República (Aníbal Cavaco Silva), que estariam «publicados em vários sítios da Internet». Terá procedido, posteriormente, à criação de regras de alarmística associadas a estes três números de contribuinte, que lhe terão permitido testar a exequibilidade do mecanismo.

Quando indagado quanto à eventualidade de existirem outros contribuintes na alarmística, para além dos três que tinha referido, JMO assegurou que não existiam. Esta declaração difere da informação que comunicou à DSAI, a 24 de fevereiro de 2015, onde o próprio informava acerca dos quatro elementos que constituíam a "lista VIP", onde se incluía o Secretário de Estado dos Assuntos Fiscais (DOC 9b).

Questionado sobre se o sistema de alarmística, enquanto funcionou, produziu alguns alertas, JMO disse ter havido dois alertas, um em relação ao acesso a dados fiscais do Primeiro-Ministro e outro a dados do Presidente da República. Sobre a atuação adotada subsequentemente aos alertas, JMO assegurou que não fez nada com os alertas, nem os comunicou à DSAI por se tratar de testes, tendo-os destruído.

A versão apresentada por JMO é desmentida cabalmente pelas provas documentais já detidas nessa altura pela CNPD, na medida em que existem as comunicações feitas por JMO à DSAI, nos dias 6 e 28 de novembro (DOCs 8d e 8e), referindo expressamente a implementação do sistema de alarmística. Por outro lado, na comunicação de 24 de fevereiro para a DSAI, JMO assume ainda o pleno funcionamento do sistema (DOC 9b).

JMO forneceu uma fotocópia da Informação ASI/238/2014 a partir do documento original, que estava arquivado no seu gabinete (DOC 11). Verificando-se que nesse documento, que lhe tinha sido entregue em 15 de outubro de 2014 por despacho de GMD, estava aposto o despacho original do Diretor-Geral, de 23 de fevereiro de 2015, questionou-se JMO como poderia o Diretor-Geral ter despachado no original que estava na posse de JMO.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

Explicou que no dia 23 de fevereiro de 2015, foi chamado ao Diretor-Geral levando consigo o documento, tendo por isso o Diretor-Geral inscrito o despacho de revogação no documento original, o qual ficou com JMO.

Nessa medida, é incompreensível que, sendo conhecedor em primeira mão do despacho que ordena o cancelamento do procedimento de alarmística, JMO no dia seguinte não só não informe a DSAI desta revogação, como ainda forneça informações e justificações sobre a composição da lista VIP (DOC 9b).

No âmbito das diligências realizadas, foram recolhidos dois *e-mails* (DOC 10) remetidos por JMO, com marca de "confidencial", tendo como assunto o NIF 177142430 (NIF do Primeiro-Ministro, Pedro Passos Coelho), datados de 24 de fevereiro de 2015 e dirigidos a GMD.

Num primeiro *e-mail*, das 12:45, JMO informa GMD dos utilizadores (através do *userID*) que acederam a dados do contribuinte acima indicado, através da aplicação *SEFWeb*, entre o período de 1 de outubro de 2013 e 26 de setembro de 2014 (DOC 10).

Num segundo *e-mail*, das 15:46, JMO remete a GMD «a identificação dos utilizadores assinalados nos *logs*», fazendo corresponder o nome e local de trabalho dos funcionários aos respetivos *userID*, à exceção de um (vp10366) ainda «a identificar» (DOC 10).

Questionado JMO sobre o contexto destes *e-mails*, disse que, não encontrando a comunicação de GMD a solicitar a informação, muito provavelmente tal foi feito por telefone.

Questionada GMD sobre o seu pedido de informação a JMO, confirmou não ter qualquer registo de comunicação eletrónica, embora não se lembrasse se a tinha apagado ou se teria feito o pedido por telefone.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

Sobre as razões para fazer tal pedido a JMO, relativamente a eventuais acessos aos dados do Primeiro-Ministro, em fevereiro de 2015, quando o processo de auditoria sobre esses acessos já tinha sido concluído em 2014, GMD afirmou relacionar-se esta pesquisa com notícias sobre dados da Segurança Social de Pedro Passos Coelho, porque «estavam a dizer que a informação tinha saído da AT».

Indagada sobre se o pedido lhe tinha sido dirigido pela DSAI no âmbito de uma nova auditoria, esclareceu que o pedido lhe tinha sido feito pelo Diretor-Geral da AT, António Brigas Afonso, que lhe terá perguntado «se a AT tinha dados da Segurança Social».

Solicitada para apresentar o pedido do Diretor-Geral, no qual se baseou para pedir a JMO para fazer aquela pesquisa, disse que o mesmo tinha sido feito telefonicamente pelo Diretor-Geral, não tendo sido formalizado por escrito.

Solicitada a apresentar a sua resposta ao Diretor-Geral, GMD disse que não respondeu por escrito e que aproveitou «um dia em que ele passou por cá – ele tem um gabinete aqui - e dei-lhe o *print* em mão».

GMD foi de novo questionada quanto à existência de alguma iniciativa interna conducente ao estabelecimento de um sistema de alerta, tendo admitido desta vez que JMO fez uma informação que foi para o Diretor-Geral, para criar um «alerta alarmista», quando os funcionários acedessem «a determinados dados críticos». Nas suas palavras, JMO terá seguido os «princípios e orientações do Garnten Group» nesta matéria.

GMD foi vaga quanto ao seu próprio envolvimento, dando a entender que não estava muito familiarizada com o conteúdo da proposta e o seu seguimento. No entanto, acabou por reconhecer que a informação circulou através do seu Gabinete de SDGSI, embora tenha afirmado que a Informação ASI/238/2014 não ficou nele arquivada.

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

Sobre o desenvolvimento dessa proposta, GMD afirmou não saber *«se o DG decidiu avançar com isto»*. Foi apenas perentória a declarar que *«sabe que o DG mandou para a DSAI»*. GMO assevera que ela *«não fez nada no sistema»*.

Questionada sobre qual foi a decisão do Diretor-Geral relativamente à proposta de JMO, disse não ter «conhecimento que houvesse despacho favorável» nem teve «conhecimento que qualquer procedimento fosse levado à prática», e GMD rematou: *«o Dr. José Morujão disse-me mesmo que não tinha sido feito nada»*.

Finalmente, faz-se nota que foi efetuada uma análise dos *logs* de acesso à aplicação de IRS realizados entre 9/5/2014 e 26/9/2014 para o Presidente da República e para o Primeiro-Ministro, recolhidos no dia 16 de março de 2015 pela equipa da CNPD, e que consta das provas documentais (DOC 6). Estes registos foram confrontados com a lista de utilizadores comunicada à DSAI (DOC 7), para efeito de auditoria, por acessos aos dados daqueles titulares de órgãos de soberania. Esta lista foi também confrontada com os nomes dos utilizadores que acederam através do SEFWeb aos dados do Primeiro-Ministro (DOC 10). Constatou-se o seguinte:

- Dos *logs* de acesso aos dados de IRS do Primeiro-Ministro, realizados entre 9/5/2014 e 26/9/2014 constam utilizadores que apesar de terem acedido à informação não figuram na lista comunicada à DSAI;

- Dos *logs* de acesso aos dados de IRS do Presidente da República, uma pesquisa efetuada no dia 24/11/2014 pelas 12:34:08, foi comunicada à DSAI a 28 de novembro, em alegado resultado da alarmística;

- Dos *logs* de acesso aos dados de IRS do Presidente da República, uma pesquisa efetuada no dia 25/11/2014, pelas 14:22:47, não foi comunicada à DSAI;

- Dos 33 utilizadores constantes na lista comunicada à DSAI por acesso aos dados do Primeiro-Ministro, 3 são claramente utilizadores externos;

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- Os 7 utilizadores constantes do *e-mail* enviado por JMO para GMD relativo ao acesso aos dados do Primeiro-Ministro, no período compreendido entre 01/10/2013 e 26/09/2014, com exceção de um utilizador (nq57057), não constam na listagem enviada para a DSAI (DOC 10).

Não foi possível identificar um padrão que permitisse perceber o critério para a comunicação dos acessos, sendo que, compete à DSAI avaliar a sua legitimidade.

Não poderá terminar-se o presente relatório sem fazer nota que JMO e GMD prestaram uma colaboração deficiente, tendo mesmo sido evasivos, incongruentes e contraditórios, induzindo a equipa em erro. Esta atitude implicou que a equipa tivesse de realizar diligências acrescidas, com desnecessário dispêndio de recursos e tempo.

*

Foram recolhidos os seguintes documentos:

- (DOC 1) Lista de perfis da aplicação de Gestão de Utilizadores;
- (DOC 2) Lista de utilizadores com perfil de acesso a dados tributários;
- (DOC 3) Cópia da Política de Segurança da Informação da Administração Fiscal e Aduaneira;
- (DOC 4) Cópia da Política de Classificação da Informação – Carta de Princípios;
- (DOC 5) Protocolo de cooperação entre a AT e a SS;
- (DOC 6) Logs de acesso à aplicação de IRS para o Presidente da República e Primeiro-Ministro entre 16/03/2014 e 16/03/2015;
- (DOC 7) Lista de utilizadores que efetuaram acessos a dados do Primeiro-Ministro entre 01/01/2014 e 26/09/2014;
- (DOCs 8 e 9) Autos de Apreensão;

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

- (DOC 10) Comunicação de JMO para GMD relativo a acessos via SEFWeb aos dados do Primeiro-Ministro;
- (DOC 11) Informação ASI/238/2014 com despacho do Diretor-Geral de 23 de fevereiro;
- (DOC 12) Logs do servidor de correio eletrónico (Microsoft Exchange) relativos à caixa de correio institucional de JMO e ASI, que referiam a expressão "238" no assunto da mensagem;
- (DOC 13) Logs do servidor de correio eletrónico (Microsoft Exchange) relativos à caixa de correio institucional de GMD, que referiam no assunto da mensagem Informação n.º ASI-238/2014 e Pedido de Informação Portal das Finanças.

Lisboa, 27 de março de 2015

Isabel Cristina Cruz

Vitor Bernardo

Clara Guerra

Marta Jacinto

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt