COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Autorização n.º 7087/2015

I. Pedido

O Centro Nacional de Cibersegurança (CNCS), através do Gabinete Nacional de Segurança, veio notificar à Comissão Nacional de Proteção de Dados (CNPD) um tratamento de dados pessoais com a finalidade de gestão e análise de incidentes de cibersegurança e ciberataques.

A informação é recolhida de forma indireta, junto de entidades da administração pública e de quaisquer entidades, públicas e privadas, detentoras de infraestruturas críticas, as quais procedem à comunicação de eventos ao CNCS, sempre que considerem que a informação registada pelos seus equipamentos de deteção de intrusão (IPS/IDS[1]) é relevante.

Entre a informação recebida, o CNCS fará o tratamento do dado pessoal "endereço de IP (*Internet Protocol*)", relativamente aos IPs públicos.

Com o acervo recolhido, o CNCS pretende analisar a informação e detetar tendências e padrões. Com base nessa análise, são elaborados e difundidos relatórios, sem dados pessoais.

[1] IPS - *Intrusion Prevention System e* IDS – *Intrusion Detection System*

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

A comunicação de eventos ao CNCS realiza-se através de redes de comunicação privadas, nos termos de protocolo de cooperação a celebrar entre o CNCS e cada uma das entidades.

Está ainda previsto que o CNCS possa comunicar dados, incluindo através de transferências internacionais, no âmbito da articulação e cooperação com entidades nacionais e estrangeiras, de acordo com a prossecução da sua missão e conforme disposto na lei.

O CNCS está ainda obrigado a comunicar à Polícia Judiciária *«os factos de que tenha conhecimento relativos à preparação e execução de crimes»* (cf. Decreto-Lei n.º 69/2014, de 9 de maio).

II. Apreciação

O tratamento de dados pessoais[2] aqui em análise diz essencialmente respeito à recolha e posterior tratamento pelo CNCS do endereço de IP. O endereço IP é um identificador de uma determinada ligação à Internet, juntamente com a data, hora e duração da ligação, e é qualificado legalmente como um dado de «*tráfego*», conforme definição da alínea *d)* do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto.

[2] Embora o CNCS não detenha, por si só, a capacidade para identificar diretamente o titular dos dados, o facto de o endereço de IP tornar identificável, mesmo que somente por terceiro, o titular, já é suficiente nos termos da LPD e do Considerando 26 da Diretiva de Proteção de Dados 95/46/CE para integrar o conceito de dados pessoais.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Nessa medida, o endereço de IP adquire uma natureza sensível, porque atinente à vida privada dos indivíduos, tal como reconhecido pelo Tribunal de Justiça da União Europeia[3].

Por outro lado, além do endereço de IP, é ainda possível que nos pacotes de dados monitorizados venham contidos outros dados pessoais, recolhidos fortuitamente.

Assim sendo, por estarem em causa dados sensíveis, na aceção do n.º 1 do artigo 7.º da Lei n.º 67/98, de 26 de outubro – Lei de Proteção de Dados Pessoais (LPD), há que encontrar neste artigo o fundamento de legitimidade para o tratamento de dados.

O Decreto-Lei n.º69/2014, de 9 de maio, estabelece como missão do CNCS *«contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais».* (cf. n.º 2 do artigo 2.º).

Na prossecução da sua missão, o CNCS tem como competência *«desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques»* (cf. n.º 1 alínea *a)* do artigo 2.º-A do diploma acima citado).

[3] Ponto 27 do Acórdão de 8 de abril de 2014, Processos C-293/12 e C-594/12.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

A gestão e análise da informação resultante de eventos registados nos equipamentos de deteção de intrusão são, por conseguinte, ações imprescindíveis ao cumprimento da missão do CNCS e emanam diretamente das competências que lhe estão legalmente conferidas.

Tal missão só poderá ser alcançada com sucesso em articulação e colaboração com as entidades nacionais públicas e com os operadores de infraestruturas críticas que comunicam ao CNCS os incidentes de cibersegurança e ciberataques.

Por isso, o fundamento de legitimidade para este tratamento de dados só pode assentar em «*motivos de interesse público importante*», o qual é notório e, pelas razões acima expostas, se revela «*indispensável ao exercício das atribuições legais ou estatutárias do seu responsável*», em conformidade com o n.º 2 do artigo 7.º da LPD.

Os dados tratados – endereço IP e informação conexa à ligação - são adequados à finalidade declarada (cf. alínea *c)* do n.º 1 do artigo 5.º da LPD). Quanto a outros dados pessoais que possam casualmente ser recolhidos entre a informação constante dos pacotes de dados, devem ser de imediato eliminados, desde que sejam inteligíveis como dados pessoais e não sejam estritamente necessários para a análise do incidente em causa.

No que diz respeito às comunicações de dados a terceiros, considera-se que elas encontram enquadramento legal nas competências específicas do CNCS, designadamente nas disposições conjugadas das alíneas *e)* e *i)* do n.º 1 e no n.º 2 do artigo 2.º-A do Decreto-Lei n.º 69/2014, de 9 de maio.

Acresce que em relação às transferências internacionais de dados para Estados ou organizações terceiras, atendendo a que o ciberespaço é por natureza transnacional

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

e, por isso, se afigura necessário o intercâmbio de informações relativas a incidentes de cibersegurança e ciberataques com múltiplos e diferenciados intervenientes, entende-se que esses fluxos transfronteiriços encontram legitimidade na alínea *c)* do n.º 1 do artigo 20.º da LPD, na medida em que são legalmente exigidos «*para a protecção de um interesse público importante*».

Todavia, deve o CNCS ponderar da necessidade de comunicar dados pessoais a terceiros, devendo abster-se de o fazer a menos que tal seja efetivamente relevante para o fim em vista.

Sempre que houver uma colaboração mais estreita e regular com alguma organização internacional ou autoridade competente de um Estado terceiro, deve a comunicação de dados radicar preferencialmente num acordo escrito.

Quanto à forma de recolha dos dados, junto das entidades da administração pública e outros operadores de infraestruturas críticas, a ser regulada por protocolo, deverá o texto do clausulado ser submetido à apreciação da CNPD.

Relativamente à pretensão de manter os dados pelo prazo de dez anos, a qual não foi justificada, mesmo admitindo-se que o fim de análise de padrões e tendências pudesse beneficiar de um período mais alargado, considera-se um prazo de conservação excessivo, principalmente tendo em conta a dinâmica e a atualidade do próprio fenómeno. Consequentemente, a CNPD entende fixar um prazo máximo de 5 anos, nos termos da alínea *f)* do n.º 1 do artigo 23.º da LPD.

Deve ainda o CNCS tomar as medidas de segurança, técnicas e organizacionais, adequadas, conforme exigido pelos artigos 14.º e 15.º da LPD.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

III. Conclusão

Assim, a CNPD autoriza o tratamento de dados nas condições acima fixadas, consignando-se nos termos e para os efeitos do disposto na alínea a) do n.º 1 do artigo 28.º e do n.º 1 do artigo 30.º da Lei n.º 67/98, de 26 de Outubro, o seguinte:

Responsável pelo tratamento: Centro Nacional de Cibersegurança /Gabinete Nacional de Segurança.

Finalidade: gestão e análise de incidentes de cibersegurança e ciberataques;

Categorias de dados tratados: endereço IP e informação conexa da comunicação;

Forma do exercício do direito de acesso: por escrito, junto do responsável;

Prazo máximo de conservação dos dados: 5 anos;

Interconexões de tratamentos: não há.

Comunicações a terceiros: Entidades nacionais e da União Europeia intervenientes na área da cibersegurança, nos termos legalmente admitidos;

Transferências de dados para países terceiros: Organizações internacionais e entidades de Estados terceiros competentes na área da cibersegurança.

Lisboa, 21 de julho de 2015

Filipa Calvão (Presidente)