PRIVACIDADE DIGITAL

SABER

O crescimento dramático da internet nos últimos vinte anos apresentou-nos novos desafios em matéria de direitos humanos; especificamente, no que diz respeito ao equilíbrio entre aqueles que são os direitos da liberdade de imprensa e os da liberdade de expressão por um lado, e por outro lado, o direitos à privacidade e proteção de dados (informação).
Pesquisar o próprio nome num motor de busca (ex: google), mesmo que nos consideremos desconhecidos, pode mostrar numa variedade de resultados sobre cada um, desde as nossas páginas nas redes sociais (ex: facebook), noticias ou outras formas de informação.
A maioria das pessoas tem uma identidade digital composta de fragmentos do passado e do presente, que permanecem guardadas ao longo do tempo. Esta identidade é usada por outros intervenientes na internet, intencionalmente ou não, para fins dos quais podemos não ter conhecimento (ex: fins comerciais).
As revelações de Edward Snowden em 2013 sobre os programas de vigilância operados pela Agência de Segurança Nacional (NSA) dos EUA e pelo GCHQ[1] (Quartel General de Comunicações Governamentais) do Reino Unido aumentaram as preocupações com a proteção do nosso direito à privacidade e à protecção de dados na Europa.
Tanto o direito a uma vida privada como o direito à protecção de dados estão protegidos pela legislação comunitária da UE e pela Convenção Europeia dos Direitos Humanos. Porém estes direitos não são absolutos – o direito à privacidade e à protecção de dados pode ser restringidos em determinadas circunstâncias.
Ao explorar estas excepções, os programas de vigilância governamentais (como revelado por Snowden nestas instâncias) invocam motivos de segurança nacional para justificar as invasões à privacidade dos cidadãos. As restrições aos direitos de proteção são difíceis de questionar ou debater, pois a informação sobre estas limitações é mantida em segredo.
A evolução gradual do “direito a ser esquecido” tem também levantado sérias questões sobre qual o papel das empresas privadas em decidir quando um direito foi violado.

COMPREENDER

O direito à privacidade e o direito à protecção de dados estão protegidos pela Carta dos Direitos Fundamentais da UE nos artigos 7º e 8º, respectivamente. O direito a uma vida privada também está protegido no espaço Europeu e em todos os países da União Europeia nos termos do artigo 8º da Convenção Europeia dos Direitos Humanos. A

---

[1] www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

protecção de dados é regulamentado em toda a UE no âmbito da Directiva de Protecção de Dados, aprovada em 1995, que exigia aos Estados Membros a aprovar leis nacionais em matéria de protecção de dados.

A Directiva de Protecção de Dados de 1995 garante que os indivíduos tenham direitos sólidos

sobre o processamento e controle de dados que lhes dizem respeito, incluindo o direito de se opor ao tratamento desses dados e o direito de acesso aos mesmos. O "controlador" dos dados deve garantir que a informação é recolhida para "fins específicos, explícitos e legítimos," e deve fazer todos os esforços para assegurar que os dados são precisos e, se não forem, corrigi-los ou apagá-los. No entanto, a Directiva de Protecção de Dados, impõe a obrigação dos Estados Membros em provisionar determinadas exceções para casos de interesse público, por exemplo, essas normas de proteção de dados não se aplicam em casos de expressão jornalística, artística ou literária.

Um acórdão recente do Tribunal de Justiça Europeu declarou que, "o direito à protecção de dados não é (…) um direito absoluto, mas deve ser considerado em relação ao papel que desempenha na sociedade,"[4] e deve ser medido segundo o princípio da proporcionalidade.[5] A liberdade de expressão, em particular, entra muitas vezes em conflito com o direito à protecção de dados visto ser outro direito fundamental, mas em contraste com a proibição da tortura ou da escravidão, não é absoluto pois tem que ser "visto em relação ao seu propósito social."

O regime de protecção de dados da UE também está a passar por um processo de revisão. Em 2012, a Comissão Europeia propôs um novo regulamento que procura compatibilizar a forma como os diferentes Estados Membros lidam com a proteção de dados, incluindo, explicitamente, o direito de ser esquecido e obrigando as empresas não-europeias que oferecem serviços aos europeus a agir em conformidade com as regras de privacidade de dados da UE.[2]

QUANDO É QUE MEUS DADOS PODEM SER RECOLHIDOS?

- Os dados que forneces só podem ser processados com base num dos seguintes critérios: o teu consentimento, serem necessários para um contrato, os teus interesses vitais, os interesses legítimos de outros (a não ser que os teus direitos fundamentais se sobreponham esse interesse legítimo), ou sempre que seja do interesse público.

---

[2] ec.europa.eu/justice/data-protection/

- Os dados sensíveis têm requisito mais rigorosos para que um consentimento seja claro, e não permitida a recolha de certos dados para estabelecer um contrato (ex: de trabalho). Dados sensíveis incluem informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical ou informações sobre saúde ou vida sexual.

- Devem ser colectados legalmente; isto é, não só que exista uma lei específica que permite um órgão governamental ou empresa recolher os teus dados, mas também que essa lei tem de servir um dos propósitos enumerados na Diretiva de Protecção de Dados ou para os direitos e liberdades de outros. Tais leis têm de se provar necessárias no contexto de uma sociedade democrática, querendo isto dizer que corresponde a uma necessidade social premente e o processamento de dados é proporcional ao propósito que o justifica.

- A finalidade da recolha dos dados deve ser especificamente e visivelmente definido antes de estes serem coletados. A recolha de dados para fins não especificados é ilegal. A transferência de dados a terceiros requere um base de enquadramento jurídica.

- Só devem ser recolhidos os dados que são adequados, pertinentes e não-excessivos para determinada finalidade e devem ser escolhidos com base no objetivo que foi declarado. A pessoa que coleta dados deve verificar se estes são correctos e atualizados. Muito importante é que os dados não devem ser retidos pelo coletor de uma forma que permita que a pessoa seja identificada por mais tempo do que é necessário para os fins da recolha. No entanto, os dados podem ser mantidos por mais tempo, mas só se forem tornados anónimos.

- Quem tiver os teus dados deve manter-te informado sobre como estes são utilizados e, tanto quanto possível, deve actuar prontamente para cumprir os teus requisitos para com o tratamento dos teus dados.

- Os titulares dos teus dados têm a obrigação de proteger a segurança e a confidencialidade desses dados. Os fornecedores de telecomunicações são obrigados a dizer-lhe se a segurança dos teus dados foi violada.

Lir mais: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

QUE DIREITOS TENHO NO ÂMBITO DA DIRECTIVA EUROPEIA DE PROTECÇÃO DE DADOS?

Tens o direito a:

- Ser informado se qualquer pessoa ou empresa tem os teus dados pessoais nos seus arquivos (web site, bases de dados, fornecedores de serviços, etc.);
- Corrigir ou apagar os teus dados, se essa informação estiver incompleta ou incorrecta;
- Ser informado por inteiro e dar o teu consentimento, se um site desejar armazenar e recuperar informações do teu computador ou para seguir as tuas actividades quando estás está online;
- Comunicação online confidencial (ex: e-mails);
- Ser notificado se os teus dados pessoais retidos por um fornecedor de serviços tenham sido perdidos, roubados ou divulgados de qualquer forma, e a tua privacidade está susceptível de ser prejudicada;
- Que não te seja enviada publicidade não solicitada (spam).

EUROPEAN ALTERNATIVES

This project is funded by the Fundamental Rights and Citizenship programme of the European Union

CITIZENRIGHTS
A project by European Alternatives