

Plataformas digitais de serviço público e a prova digital

Luis Borges Gouveia, Prof. Catedrático (UFP)

Conferência Prova Digital, 29 de outubro de 2018

Auditório António Domingues de Azevedo, Lisboa



ORDEM DOS ADVOGADOS
CONSELHO REGIONAL DE LISBOA

Prova Digital

- ***qualquer tipo de informação, com valor probatório, armazenada em repositório eletrónico-digitais de armazenamento, ou transmitida em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis, sob a forma binária ou digital***
Rodrigues, B. (2009). Direito Penal Parte Especial, Tomo I, Direito Penal Informático-Digital, Coimbra, p. 722.
- ***informação passível de ser **extraída** de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também **autêntica, precisa e concreta*****
Ramos, A. (2014). A Prova Digital em Processo Penal. Chiado Editora, p. 86.

Conceitos associados

- **Rastro** digital
 - produzido por atividade direta no ecossistema digital
- **Pegada** digital
 - referencias existentes no ecossistema digital
- Tipo de **materiais** para efeito de prova digital
 - conteúdos e metadados
- **Fiabilidade** de conteúdos e de metadados
 - reprodutibilidade e verificabilidade
- **Fidedignidade** de conteúdos e de metadados
 - qualidade dos dados e da informação
- **Informática forense**
 - recolha e preservação da prova digital

Rastro e pegada

- **Rastro**

- Produzido pelo próprio ou pela sua ação com terceiros
- Crescente mediação da atividade humana, torna cada vez mais visível o rastro, embora existam limites legais e técnicos para a sua profundidade (entendida como o período temporal e o detalhe associado – exemplos: RGPD, privacidade, entre outros)

- **Pegada**

- Produzido por terceiros e que captura de forma indireta a atividade do próprio
- A existência generalizada de sistemas de base digital torna grande a probabilidade de captura de conteúdos e metadados que envolvam, mesmo de forma indireta cada identidade em particular

- **Crescente aumento do peso da pegada, face ao rastro**

- Mais difícil de alterar pelo próprio, mas ainda de maior complexidade técnica e legal de obter
- Permite reconstituir a atividade de indivíduos e organizações por via do cruzamento de metadados de diversas fontes (complexo, mas de eficácia crescente)

Tipos de materiais

- **Conteúdos**

- Dados: o mais comum (no contexto da legislação, com diferentes nomes atribuídos como dados de tráfego, informação pessoal, dados sensível, entre outros)
- Informação: pressupõe a organização dos dados e um contexto (logo, adicionando metadados – exige o conhecimento de estruturas e normalmente o acesso a bases de dados e a dados estruturados)
- Conhecimento: pressupõe o cruzamento e comparação com dados e informação adicional aos dados e informação em análise (logo, adicionando uma componente analítica, com maior complexidade)

- **Metadados**

- Os dados que descrevem os dados
 - Proporcionam contexto
 - Exigem um nível de conhecimento técnico mais especializado
- Os dados podem ser referenciados, encriptados, anonimizados, etc. (...)
 - O jogo de proteção de dados e da sua segurança, pode adicionar elementos de dificuldade para a obtenção da prova digital

Fiabilidade e fidedignidade (questões)

- **Fiabilidade** (de conteúdos e de metadados)
 - É possível reconstituir o rastro ou obter evidência?
 - É possível identificar quem, quando, onde, como e porquê?
- **Fidedignidade** (de conteúdos e de metadados)
 - Existe uma correspondência com os elementos em estudo?
 - A informação obtida é clara, precisa, completa, concisa e simples?
- Estes elementos condicionam a recolha e preservação da prova digital (*informática forense*) e a avaliação subjetiva da prova digital

Questão de estudo

- Como podem as plataformas associadas com a administração pública e o poder executivo auxiliar na organização de informação que potencie a existência de prova digital quando e onde for necessária?
- (neste contexto) Acredita-se ser crítica a gestão da informação (de conteúdos e de metadados):
 - Tal exige uma revisão dos sistemas de informação, (ainda) mais orientados para uma prática em papel do que para o digital
 - Preparar os sistemas de informação de acordo com as necessidade de verificação da prova digital
- Dois exemplos em investigação (contexto Brasileiro)
 - A importância da segurança da informação para os portais de transparência
 - A implementação de mecanismos de controlo social para combate à corrupção

Transparência, *e-government* e segurança da informação: uma contribuição para a sua discussão no contexto do poder público

**Doutoramento em Ciências da Informação, especialidade Sistemas,
Tecnologias e Gestão da Informação
Carlos Silva, Luis Borges Gouveia (orientador)**



UNIVERSIDADE

FERNANDO PESSOA

WWW.UFP.PT

Introdução

Exemplo 1

- Propõe-se relacionar a transparência com a segurança da informação, no contexto do poder público
 - Como promover o desenvolvimento de boas práticas de modo a manter o equilíbrio entre transparência e segurança da informação
- Eficiência, eficácia, transparência, desempenho, mecanismos de controle, prestação de contas e qualidades do gasto público, passaram a estar relacionados com o digital e com o governo eletrónico (plataformas digitais)
- A Segurança da informação, enquanto preocupação de salvaguarda da informação, da sua divulgação, preservação e proteção para a minimização dos riscos, está relacionada com as atividades do poder público

Transparência

Exemplo 1

- A política de transparência pode ser considerada como a condição de acesso a toda e qualquer informação dos atos praticados pelo governo, e de como os recursos públicos são aplicados
- Um governo é considerado transparente quando há um envolvimento público, governo mais sociedade, em todos os planos e assuntos estratégicos de interesse de qualquer uma das esferas da administração
- A transparência tornou-se um dos pilares que dá sustentação à administração pública e acompanhando a tendência o Brasil baseou-se nos seguintes modelos para criar sua própria legislação:
 - *Fiscal Transparency* do FMI;
 - *Fiscal Responsibility Act* da Nova Zelândia (1994);
 - *Budget Enforcement Act* dos EUA (1990);
 - Tratado de *Maastricht* da União Monetária Europeia (1992).
- O enquadramento legal Brasileiro é o seguinte:
 - Lei Complementar Nº 101, de 04 de maio de 2000 (LRF)
 - Artigo 48 - instrumentos de transparência da gestão fiscal
 - Lei Complementar nº 131, de 27 de maio de 2009 que acrescenta novos dispositivos à LRF, entre elas: disponibilização de informação em tempo real e o prazo para o seu cumprimento nas três esferas da administração (federal, estadual e local)

Transparência e E-Government

Exemplo 1

- Os governos, na busca de melhorar os processos administrativos e operacionais, fazem uso de recursos digitais proporcionados pelas TIC e plataformas digitais, como a Internet, para a divulgação dos atos da gestão pública no intercâmbio com o cidadão
- Temas como eficiência, eficácia, transparência, desempenho, mecanismos de controle, prestação de contas e qualidades do gasto público, passaram a estar relacionados com esse processo de modernização e conseqüentemente sendo associados à constituição do governo eletrónico;
- *O e-government* possui um papel importante na democratização da informação ao cidadão e na promoção de serviços de base digital que facilitam a vida do cidadão

Transparência e Segurança da Informação

Exemplo 1

- A informação, para qualquer entidade, seja ela um órgão governamental ou uma empresa privada, é de importância fundamental e dependendo de seu valor para a organização, a sua integridade deve ser preservada
- Informação pode ser entendida como qualquer dado que tenha valor para uma pessoa ou entidade.
- A segurança da informação deve ser acautelada:
 - Naturalmente através de legislação
 - Mas também no contexto das TIC, onde a sua operacionalização é mais sensível
 - E envolver recursos humanos dos diferentes órgãos (desenvolvendo competências) e o cidadão (ações de sensibilização)

Transparência e Segurança da Informação

Exemplo 1

- A segurança proporcionada pelas TIC oferece soluções para estruturar os documentos existentes nos órgãos da administração pública
- As TICs ajudam a garantir:
 - Confidencialidade (salvaguardar os dados e identidades associadas)
 - Integridade (assegurar e proteger a correção dos dados)
 - Disponibilidade (garantir o acesso aos dados)
- A negligência na Segurança da Informação pode ocasionar:
 - Roubo
 - Perda ou alteração de dados pessoais ou empresariais, e principalmente governamentais, provocando assim prejuízos tanto financeiros, como ao Estado democrático e à soberania nacional
- A ruptura de um dos 3 aspectos críticos que são, Confidencialidade, Integridade e Disponibilidade, conhecidos como os pilares que garantem a segurança da informação, comprometem toda e qualquer informação

Considerações Finais

Exemplo 1

- A preocupação do governo com a eficácia, a eficiência, a efetividade e a *accountability* das suas ações, levaram ao interesse pelas políticas públicas de transparência
 - o uso das TICs possuem um grande potencial para o aumento da transparência, contribuindo assim para a concepção de uma nova cidadania
- Propõe-se o relacionamento da Transparência, como um componente do *e-government*, com a Segurança da Informação, como base para a sua credibilidade perante o cidadão que pretende estar informado de como atua a administração pública

O uso do governo eletrónico pelo controlo social no combate à corrupção pública no Ceará

Doutoramento em Ciências da Informação, especialidade Sistemas,
Tecnologias e Gestão da Informação
Nazaré Pinto, Luis Borges Gouveia (orientador)



UNIVERSIDADE

FERNANDO PESSOA

WWW.UFP.PT

Introdução

Exemplo 2

- No combate à corrupção generalizada na administração pública, é proposta a execução do controle social com o uso da informação disponível nos portais eletrônicos do governo brasileiro (gov.br).
- Para que o controle social aconteça, o Estado deverá promover a educação cidadã, ensinando a população sobre o seu papel fiscalizador
- Esta ação incentivará mudanças culturais no senso comum de que: ***“o que é de todos, não é de ninguém”***

Enquadramento

Exemplo 2

- Segundo os dados do IBGE/2016:
 - O Brasil tem uma população de 209 milhões de habitantes;
 - 5º maior país do mundo em extensão territorial;
 - Possui 27 Unidades fiscais e 5 570 municípios.
- A base de informação é o sistema SOU de ouvidoria do Estado do Ceará
 - Verifica-se a inexistência de Website nas 233 escolas da rede estadual
- Em muitas regiões a grande motivação para o aluno frequentar a escola é a merenda escolar e não o sistema educacional



Proposta

Exemplo 2

- A implantação de programas do E-gov com a utilização das TIC para facilitar o acesso do cidadão aos principais serviços disponíveis nos meios digitais, que são:
 - Acesso aos dados orçamentários nos quais se identifica o valor do gasto, o credor e o objeto que deu origem à despesa, que pode ser a aquisição de bens, serviços ou obras
 - Carta de serviços ao cidadão, editais de seleção para estágios, concursos, licitações, convénios, orientações e Ouvidoria (provedoria) onde podem ser registradas reclamações, denúncias, elogios e solicitações de informações

Resultado

Exemplo 2

- Website nas escolas públicas estaduais de Fortaleza, com o fim de informar aos **atores** sociais envolvidos na alimentação escolar visa dar conhecimento da realidade das despesas daquela escola
- O controle social nas escolas públicas para acompanhar a merenda escolar objeto do PNAE que alcança todo o território nacional e que em 2016 seu orçamento foi de aproximadamente 3,6 mil milhões de reais

Conclusão

Exemplo 2

- Reduzir a corrupção, requer um trabalho de parceria do Estado com a sociedade, com ações que incluam uma nova forma de organização envolvendo propostas que possam ser executadas de baixo para cima, com recurso ao e-government
- Combater a corrupção deve incluir a população, com treino para conhecer, entender e aprender a acompanhar os recursos públicos, dispondo de ferramenta tecnológica adequada aos utilizadores, independentemente dos seus perfis sociais e educacionais.

Nota biográfica: Luis Borges Gouveia

Hab., PhD, MsC, Dip – Sistemas e Tecnologias de Informação

Professor Catedrático na Faculdade de Ciências e Tecnologia da Universidade Fernando Pessoa (UFP)

Coordenador do Doutoramento em Ciências da Informação, Especialidade Sistemas, Tecnologias e Gestão da Informação (UFP)

Consultor, palestrante e autor em sistemas de informação e transformação digital

Auditor de Defesa Nacional, membro do Grupo de Reflexão sobre Resiliência Cibernética, Instituto de Defesa Nacional (IDN)

Membro da Direção Norte da Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI)

Agregação em Engenharia e Gestão Industrial pela Universidade de Aveiro (UA)

Doutoramento em Ciências da Computação pela Universidade de Lancaster (UK, ULancs)

Mestrado em Engenharia Eletrotécnica e de Computadores, pela Faculdade de Engenharia da Universidade do Porto (FEUP)

Licenciado em Matemáticas Aplicadas / Informática pela Universidade Portucalense (UPT)

Possui página na Web (<http://homepage.ufp.pt/lmbq/>)