**1º ENGCCI**
**30 mar 2012**

# Transparência Eleitoral e Respeito ao Eleitor - Para onde foi o [sigilo do] voto?


Prof. Pedro A. D. Rezende

Ciência da Computação – Universidade de Brasília


Colaboração:

Forum do Voto Seguro, CMIND

# O Sigilo do Voto

**Código Eleitoral** (desde a Lei 4737/65):

Art. 103. “O sigilo do voto é assegurado mediante as seguintes providências: …

IV emprego de urna que assegure a inviolabilidade do sufrágio e seja suficientemente ampla para que não se acumulem as cédulas na ordem que forem introduzidas”

# Testes Públicos de Segurança da Urna Eletrônica

**Tribunal Superior Eleitoral**:

Brasília, 20, 21 e 22 de março de 2012.

Parâmetros: Verificar se é possível alterar o resultado ou violar o sigilo do voto numa eleição simulada, sob condições controladas

# O Sigilo do Voto

**Código Eleitoral** (desde a Lei 4737/65):

Art. 220. “É nula a votação: ...

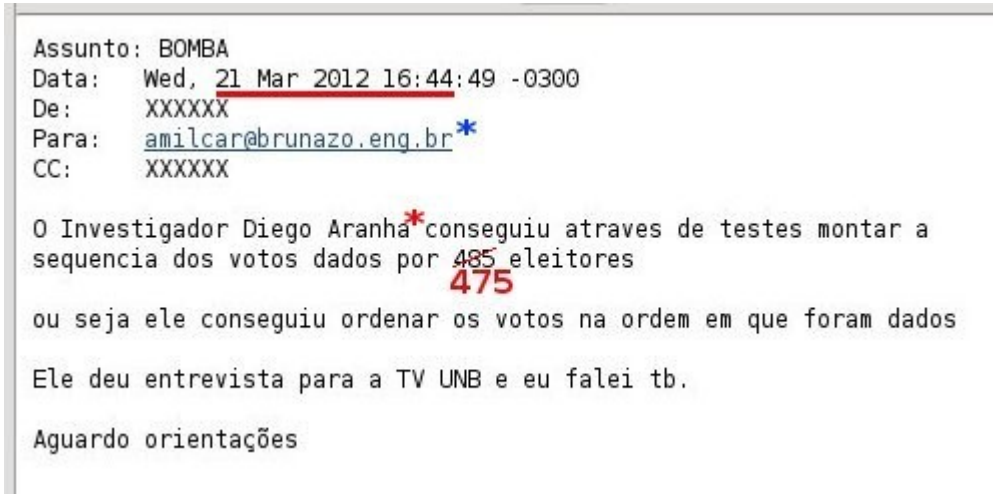
IV quando preterida formalidade essencial do sigilo dos sufrágios.”

# O Sigilo do Voto

**Código Eleitoral** (desde a Lei 4737/65):

Art. 220. “É nula a votação: ...

IV quando preterida formalidade essencial do sigilo dos sufrágios.”



Assunto: BOMBA
Data: Wed, 21 Mar 2012 16:44:49 -0300
De: XXXXXX
Para: amilcar@brunazo.eng.br*
CC: XXXXXX

O Investigador Diego Aranha* conseguiu atraves de testes montar a sequencia dos votos dados por ~~485~~ 475 eleitores

ou seja ele conseguiu ordenar os votos na ordem em que foram dados

Ele deu entrevista para a TV UNB e eu falei tb.

Aguardo orientações

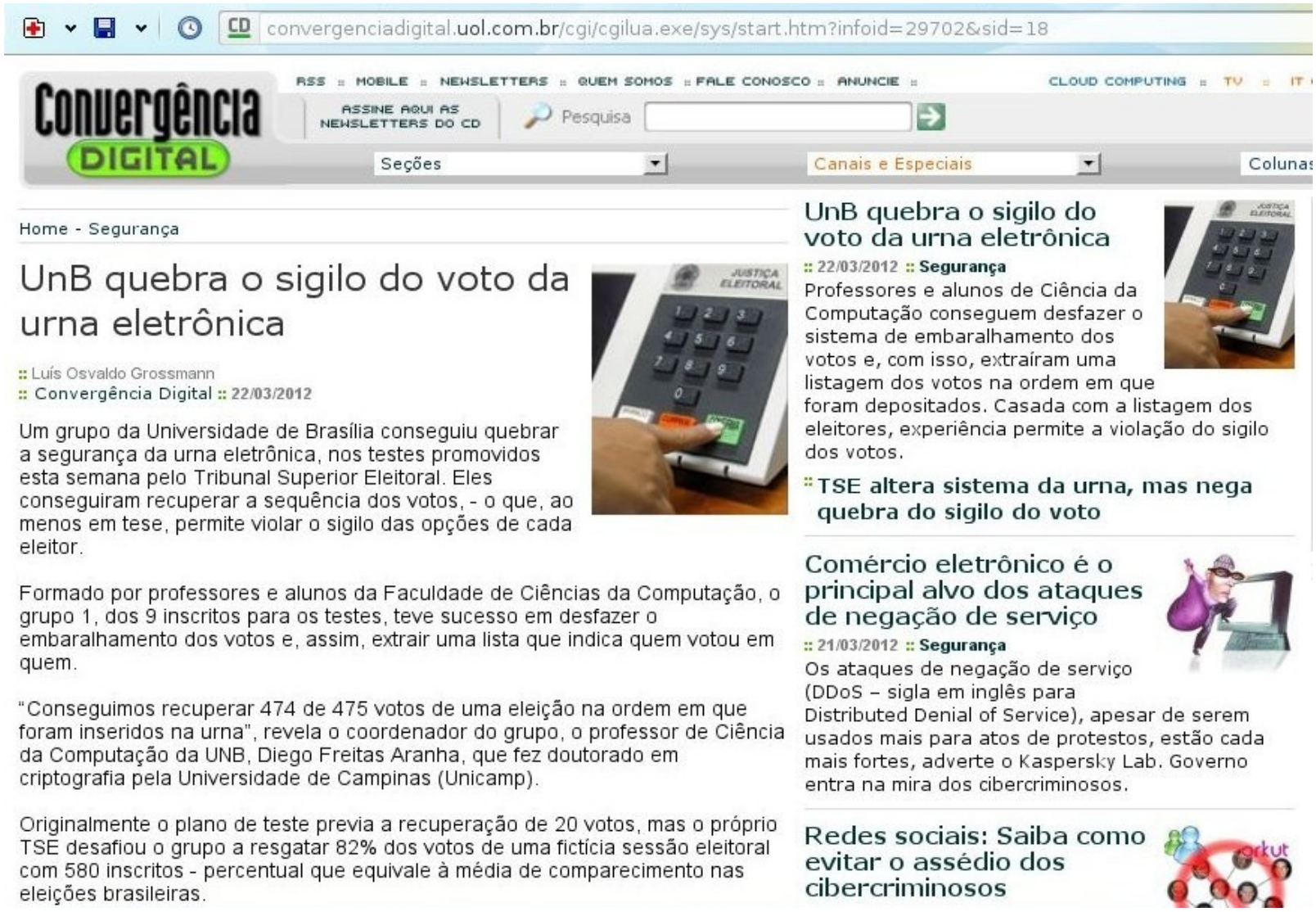
**Contexto do Furo**:

2a. Edição do “Teste Público de Segurança” da Urna (UE), promovido pelo TSE em 20, 21, 22 e 29/3/2012

* Moderador Votoseguro.org

* Líder da Equipe 1 (de 9)

# Teste Público de Segurança da Urna 2012



convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=29702&sid=18

Convergência Digital

RSS :: MOBILE :: NEWSLETTERS :: QUEM SOMOS :: FALE CONOSCO :: ANUNCIE :: CLOUD COMPUTING :: TV :: IT

ASSINE AQUI AS NEWSLETTERS DO CD

Pesquisa

Seções | Canais e Especiais | Colunas

Home - Segurança

## UnB quebra o sigilo do voto da urna eletrônica

:: Luís Osvaldo Grossmann
:: Convergência Digital :: 22/03/2012

Um grupo da Universidade de Brasília conseguiu quebrar a segurança da urna eletrônica, nos testes promovidos esta semana pelo Tribunal Superior Eleitoral. Eles conseguiram recuperar a sequência dos votos, - o que, ao menos em tese, permite violar o sigilo das opções de cada eleitor.

Formado por professores e alunos da Faculdade de Ciências da Computação, o grupo 1, dos 9 inscritos para os testes, teve sucesso em desfazer o embaralhamento dos votos e, assim, extrair uma lista que indica quem votou em quem.

"Conseguimos recuperar 474 de 475 votos de uma eleição na ordem em que foram inseridos na urna", revela o coordenador do grupo, o professor de Ciência da Computação da UNB, Diego Freitas Aranha, que fez doutorado em criptografia pela Universidade de Campinas (Unicamp).

Originalmente o plano de teste previa a recuperação de 20 votos, mas o próprio TSE desafiou o grupo a resgatar 82% dos votos de uma fictícia sessão eleitoral com 580 inscritos - percentual que equivale à média de comparecimento nas eleições brasileiras.

### UnB quebra o sigilo do voto da urna eletrônica

:: 22/03/2012 :: **Segurança**

Professores e alunos de Ciência da Computação conseguem desfazer o sistema de embaralhamento dos votos e, com isso, extraíram uma listagem dos votos na ordem em que foram depositados. Casada com a listagem dos eleitores, experiência permite a violação do sigilo dos votos.

:: **TSE altera sistema da urna, mas nega quebra do sigilo do voto**

### Comércio eletrônico é o principal alvo dos ataques de negação de serviço

:: 21/03/2012 :: **Segurança**

Os ataques de negação de serviço (DDoS – sigla em inglês para Distributed Denial of Service), apesar de serem usados mais para atos de protestos, estão cada mais fortes, adverte o Kaspersky Lab. Governo entra na mira dos cibercriminosos.

### Redes sociais: Saiba como evitar o assédio dos cibercriminosos

# Teste Público de Segurança da Urna 2012

convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=29702&sid=18

Convergência DIGITAL

RSS :: MOBILE :: NEWSLETTERS :: QUEM SOMOS :: FALE CONOSCO :: ANUNCIE :: CLOUD COMPUTING :: TV :: IT

ASSINE AQUI AS NEWSLETTERS DO CD

Pesquisa

Seções | Canais e Especiais | Colunas

Home - Segurança

## UnB quebra o sigilo do voto da urna eletrônica

:: Luís Osvaldo Grossmann
:: Convergência Digital :: 22/03/2012


Um grupo da Universidade de Brasília conseguiu quebrar a segurança da urna eletrônica, nos testes promovidos esta semana pelo Tribunal Superior Eleitoral. Eles conseguiram recuperar a sequência dos votos, - o que, ao menos em tese, permite violar o sigilo das opções de cada eleitor.

Formado por professores e alunos da Faculdade de Ciências da Computação, o grupo 1, dos 9 inscritos para os testes, teve sucesso em desfazer o embaralhamento dos votos e, assim, extrair uma lista que indica quem votou em quem.

"Conseguimos recuperar 474 de 475 votos de uma eleição na ordem em que foram inseridos na urna", revela o coordenador do grupo, o professor de Ciência da Computação da UNB, Diego Freitas Aranha, que fez doutorado em criptografia pela Universidade de Campinas (Unicamp).

Originalmente o plano de teste previa a recuperação de 20 votos, mas o próprio TSE desafiou o grupo a resgatar 82% dos votos de uma fictícia sessão eleitoral com 580 inscritos - percentual que equivale à média de comparecimento nas eleições brasileiras.

### UnB quebra o sigilo do voto da urna eletrônica


:: 22/03/2012 :: **Segurança**

Professores e alunos de Ciência da Computação conseguem desfazer o sistema de embaralhamento dos votos e, com isso, extraíram uma listagem dos votos na ordem em que foram depositados. Casada com a listagem dos eleitores, experiência permite a violação do sigilo dos votos.

:: **TSE altera sistema da urna, mas nega quebra do sigilo do voto**

**Contexto**:

Grossmann talvez acompanhe o forum Votoseguro.org

O Furo da notícia pela versão do Investigador, em 22/3, levou a voz do Investigado a falar em *código*

# TSE Nega

Declaração do Presidente do TSE ao *O Globo*

http://g1.globo.com/tecnologia/noticia/2012/03/unbdizquedescobriufragilidadenaseguranca daurnaeletronica.html

"*não houve violação da urna eletrônica durante o teste, porque os especialistas tiveram acesso a* ***um código****… Foi dentro de um ambiente controlado. Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte.… O eleitor pode ficar tranquilo que não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor*", disse Lewandowski

# Como decodificar? (1)

Tentando:

"*não houve violação da urna eletrônica durante o teste, porque os especialistas tiveram acesso a* ***um código****…*"

Alegouse que houve **quebra do sigilo do voto,** e *não* que houve **violação da urna eletrônica**. Houve quebra do sigilo do voto porque especialistas tiveram acesso a **código fonte** do software ***da*** **urna.** E *não* houve violação da urna porque especialistas *não* tiveram acesso a **código executável *na* urna**.

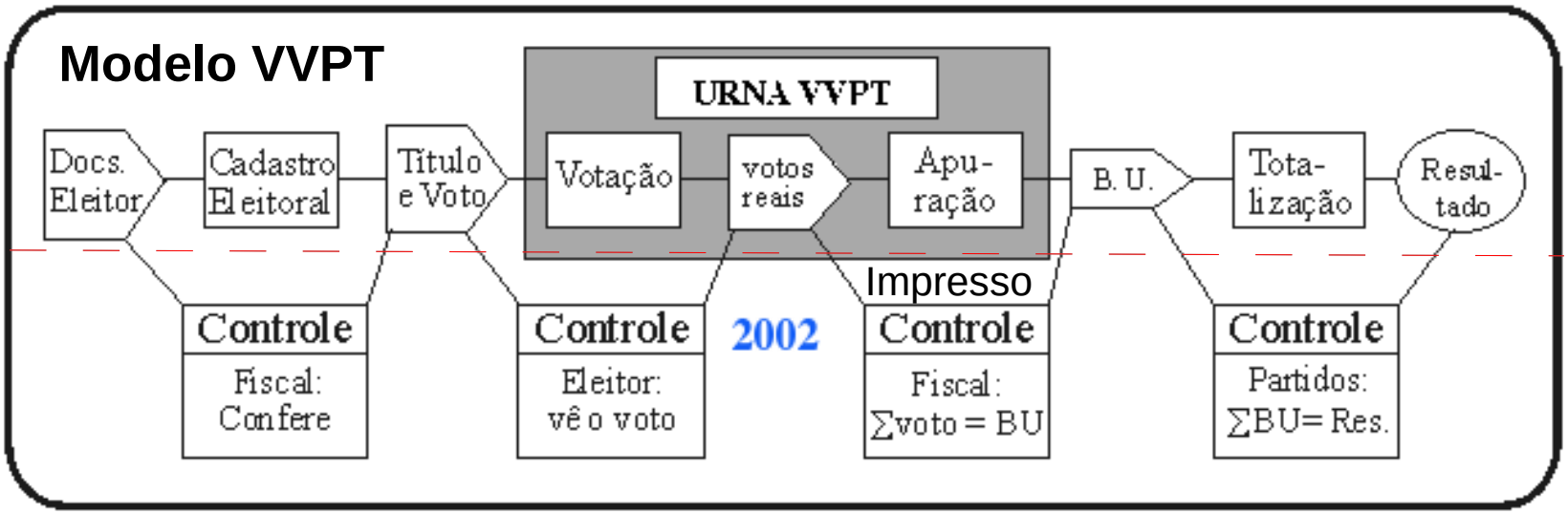
# Sistemas de Votação


Eleição Informatizada

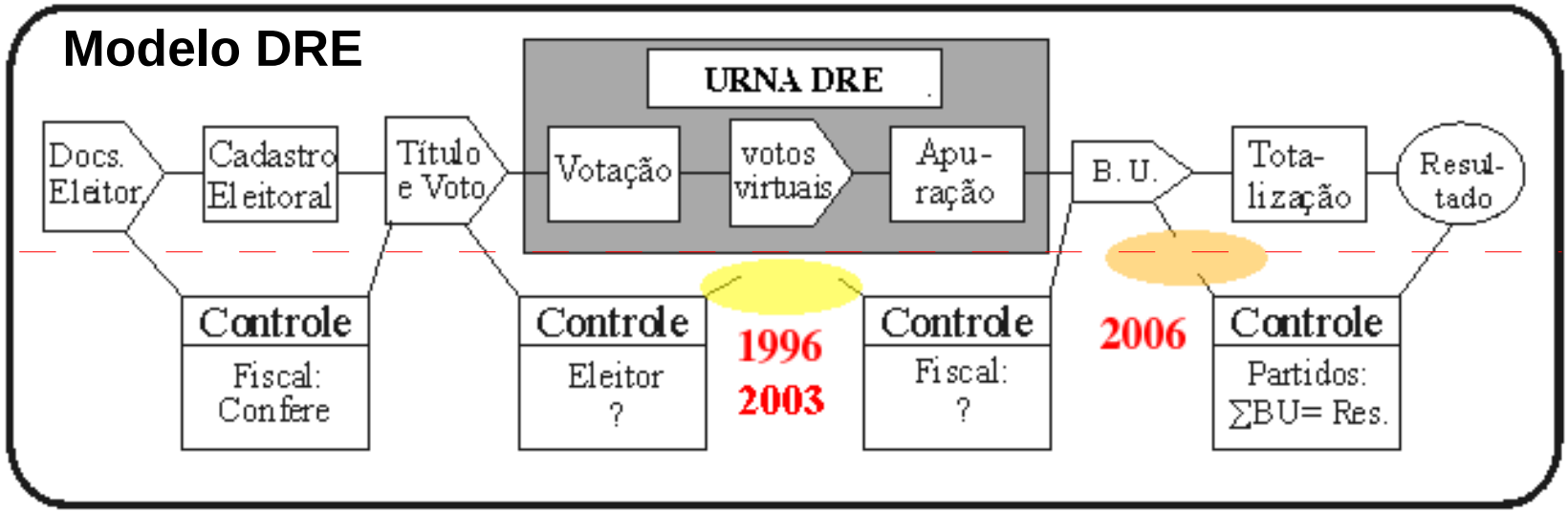
**NÃO** se resume às urnas

- Iniciase na licitação de *hardware*, programas e suporte para várias etapas e subprocessos;
- Deveria passar por **homologação** independente de componentes e subsistemas;
- Deveria incluir meios **independentes** de **verificação** dos resultados do processo.

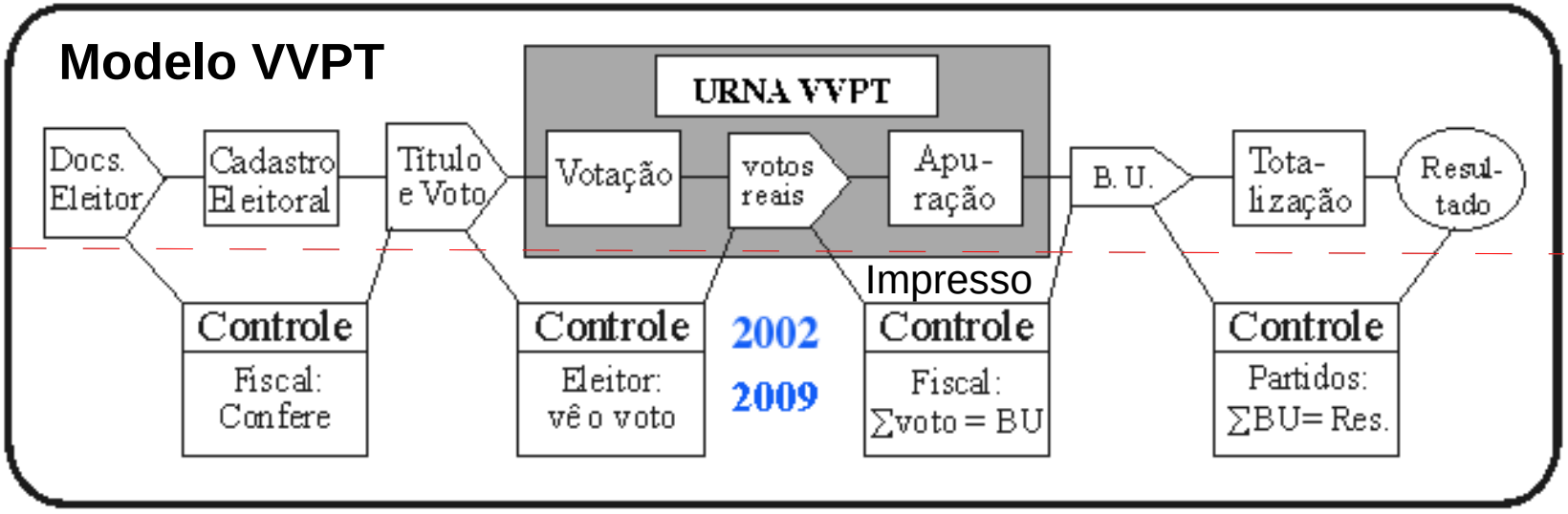
# Etapas do processo



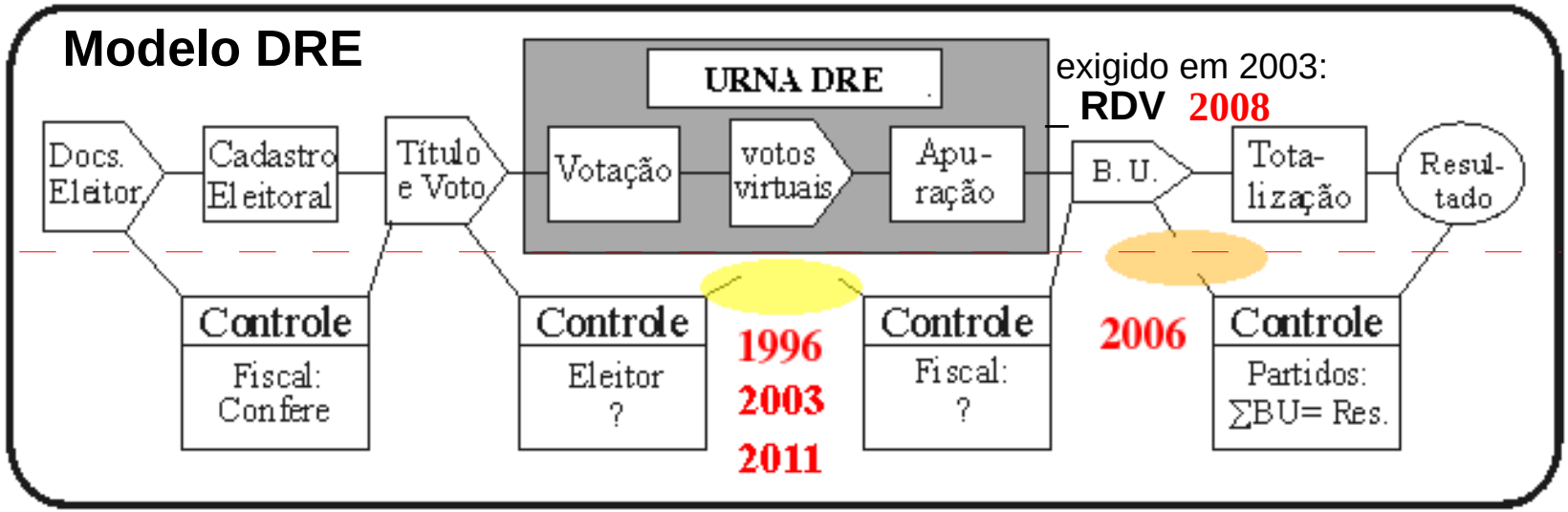

Até 2007



# Etapas do processo




2012



# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

### 1º Voto

O do 1º Eleitor a votar na seção


| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | gv | 51 | | |
| | | | | | |
| | | | | | |
| pr | 13 | | | | |
| | | | | se | 15 |
| | | | | | |

# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

### 2º Voto

O do 2º Eleitor a votar na seção


| | | | | | |
|---|---|---|---|---|---|
| | | | | se | 23 |
| | | gv | 51 | | |
| pr | 21 | | | | |
| | | | | | |
| pr | 13 | | | | |
| | | | | se | 15 |
| | | gv | 13 | | |

# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

### 3º Voto

O do 3º Eleitor a votar na seção


| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | | | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | | | | |
| | | gv | 13 | | |
| pr | 13 | | | | |
| | | | | se | 15 |
| | | gv | 13 | | |

# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

### 4º Voto

O do 4º Eleitor a votar na seção


| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | | | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | | |
| pr | 23 | | | se | 15 |
| | | gv | 13 | | |

# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

### 5º Voto

O do 5º Eleitor a votar na seção


| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

# RDV

## Registro Digital dos Votos:

O que a Equipe 1 utilizou *da* **saída normal** da urna, *em* simulação controlada, *para* a alegada quebra:

Dados representáveis numa planilha eletrônica que vai sendo gravada com os votos em posições aleatórias durante votação

Fim da Votação

5 Votantes
2 Abstenções
na seção


Saída

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

**RDV**, Log, BU da seção <

# Desembaralhamento

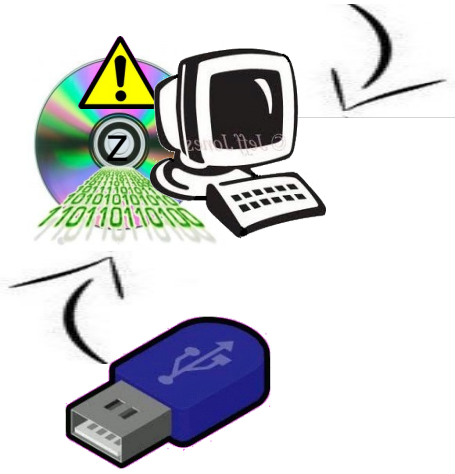
RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

Semente



| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |


| pr | 13 | gv | 51 | se | 15 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

2º Voto

| | | | | | |
|---|---|---|---|---|---|
| pr | 13 | gv | 51 | se | 15 |
| **pr** | **23** | **gv** | **13** | **se** | **23** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

3º Voto

| | | | | | |
|---|---|---|---|---|---|
| pr | 13 | gv | 51 | se | 15 |
| pr | 23 | gv | 13 | se | 23 |
| **pr** | **51** | **gv** | **13** | **se** | **15** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |


| | | | | | |
|---|---|---|---|---|---|
| pr | 13 | gv | 51 | se | 15 |
| pr | 23 | gv | 13 | se | 23 |
| pr | 51 | gv | 13 | se | 15 |
| **pr** | **23** | **gv** | **23** | **se** | **23** |
| | | | | | |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

5º Voto

| | | | | | |
|---|---|---|---|---|---|
| pr | 13 | gv | 51 | se | 15 |
| pr | 23 | gv | 13 | se | 23 |
| pr | 51 | gv | 13 | se | 15 |
| pr | 23 | gv | 23 | se | 23 |
| **pr** | **13** | **gv** | **15** | **se** | **51** |
| | | | | | |
| | | | | | |

# Desembaralhamento

RDV, Log:

O que a Equipe 1 utilizou *como entrada* de seu programa, para imprimir os votos na ordem correta:

O programa precisa refazer a mesma sequencia de posições “aleatórias” da gravação, para ler do RDV na ordem correta.

| | | | | | |
|---|---|---|---|---|---|
| pr | 51 | gv | 15 | se | 23 |
| | | gv | 51 | se | 15 |
| pr | 23 | gv | 23 | | |
| | | gv | 13 | se | 23 |
| pr | 13 | | | se | 51 |
| pr | 23 | | | se | 15 |
| pr | 13 | gv | 13 | | |

Abstenção

| | | | | | |
|---|---|---|---|---|---|
| pr | 13 | gv | 51 | se | 15 |
| pr | 23 | gv | 13 | se | 23 |
| pr | 51 | gv | 13 | se | 15 |
| pr | 23 | gv | 23 | se | 23 |
| pr | 13 | gv | 15 | se | 51 |
| | | | | | |
| | | | | | |

# Como decodificar? (2)

"*Foi dentro de um ambiente controlado. Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte.*”

No contexto desse ambiente controlado, “fonte” significa **código fonte**.

# Como decodificar? (2)

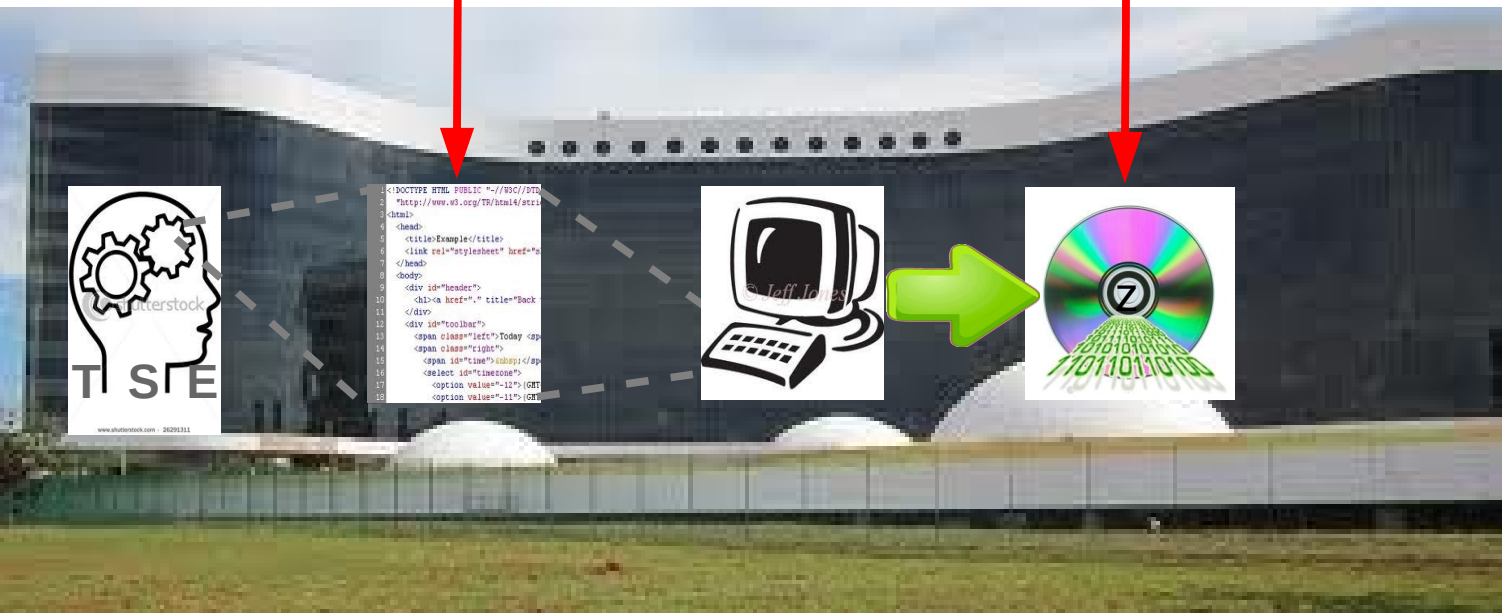
"*Foi dentro de um ambiente controlado. Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte.*"

No contexto desse ambiente controlado, "fonte" significa **código fonte** ...

# Como decodificar? (2)

"*Foi dentro de um ambiente controlado. Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte.*"

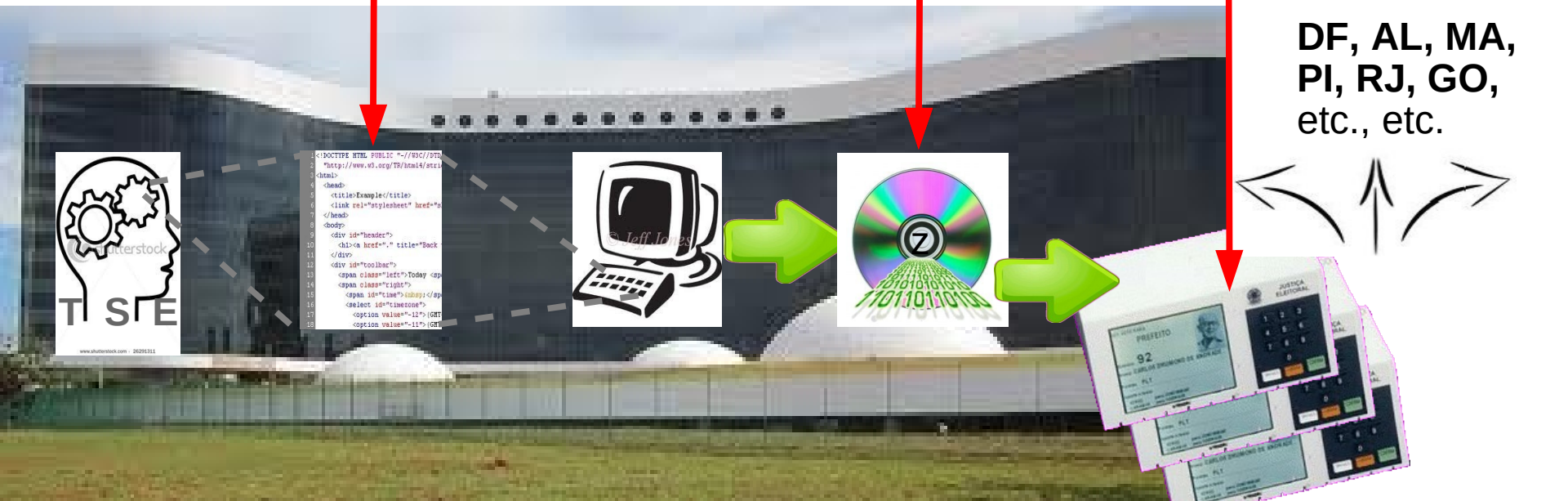
No contexto desse ambiente controlado, "fonte" significa **código fonte** do *software* da urna ...



# Como decodificar? (2)

"*Foi dentro de um ambiente controlado. Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte.*"

No contexto desse ambiente controlado, "fonte" significa **código fonte** do *software* da urna *a testar*:

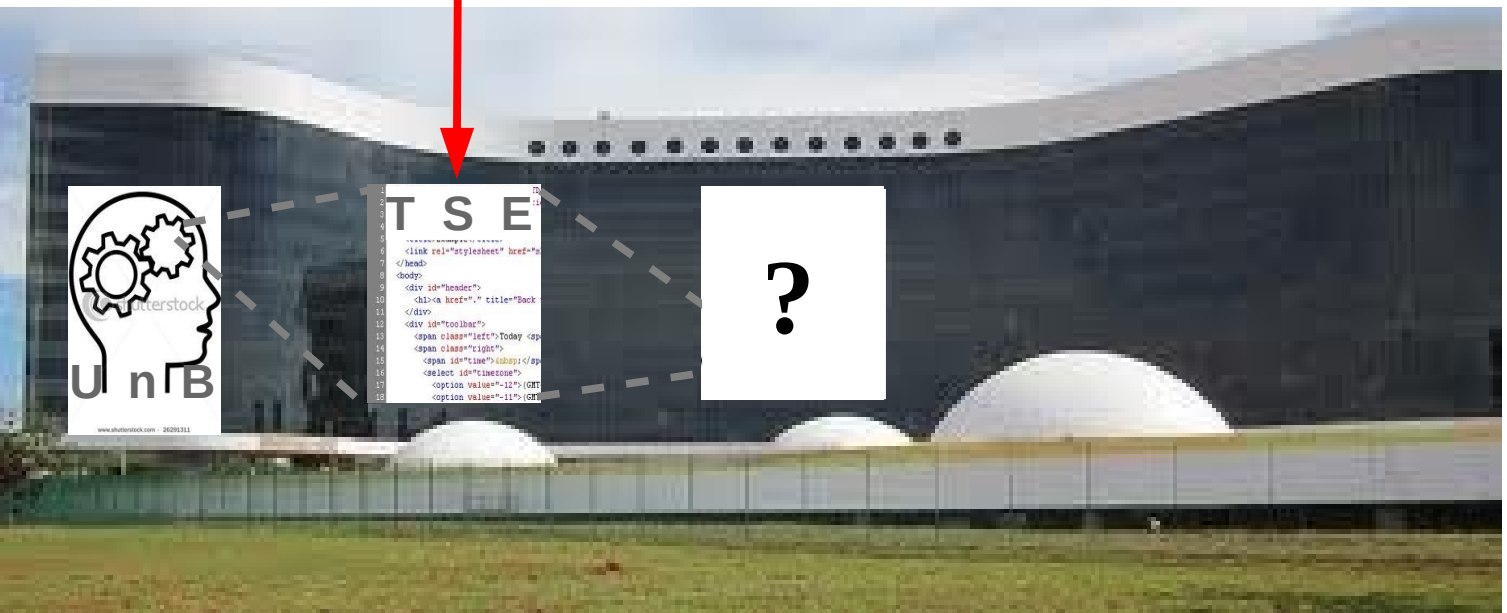


# Como decodificar? (3)

"*Foi dentro de um ambiente controlado. Isto ...*"

No ambiente controlado desses testes, “Isto” significa:

O código fonte desse software **revela** ...

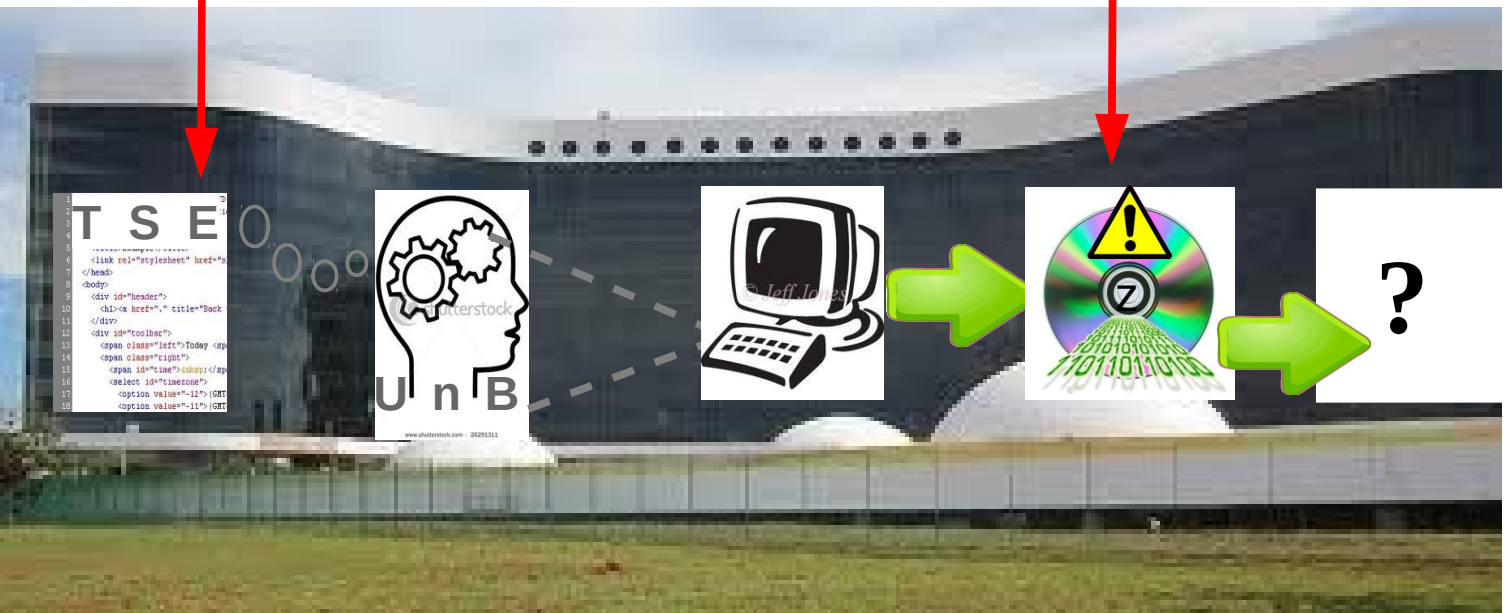


# Como decodificar? (3)

"*Foi dentro de um ambiente controlado. Isto ...*"

No ambiente controlado desses testes, “Isto” significa:

O código fonte desse software **revela** (a quem sabe), como desembaralhar RDVs ...



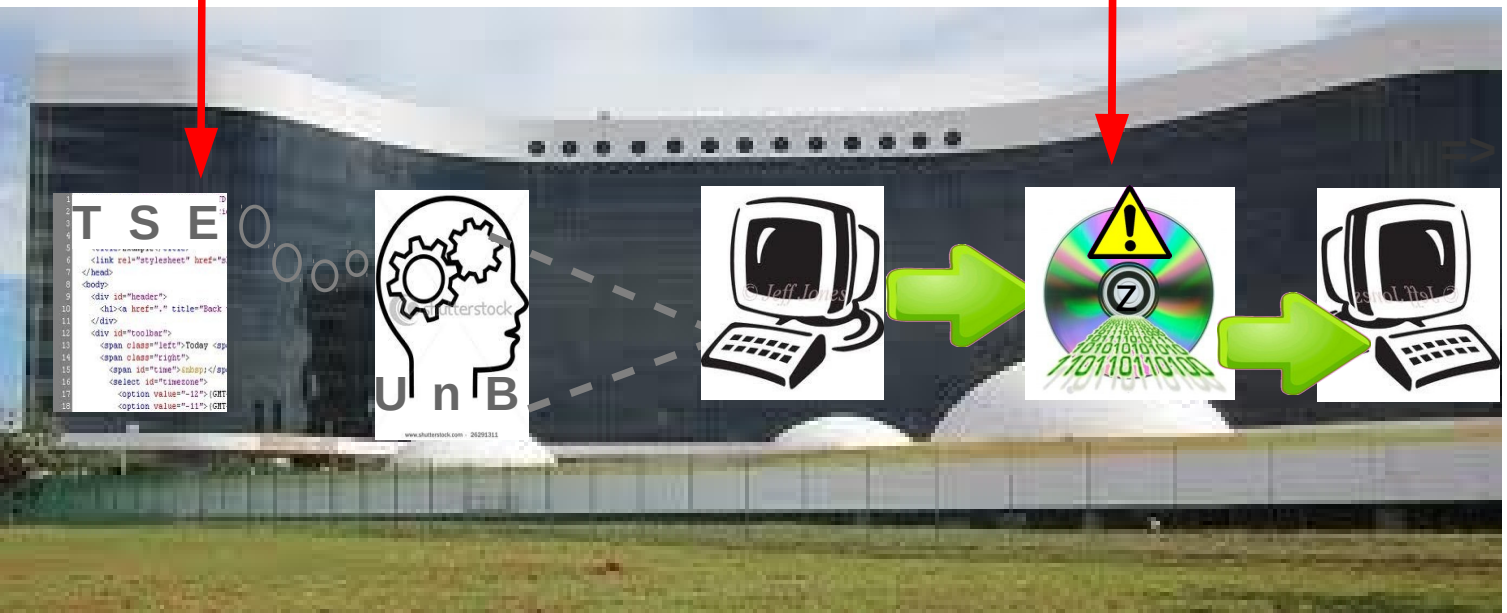
# Como decodificar? (3)

"*Foi dentro de um ambiente controlado. Isto ...*"

No ambiente controlado desses testes, "Isto" significa:

O código fonte desse software **revela** (a quem sabe),

como desembaralhar RDVs gerados por ele ...



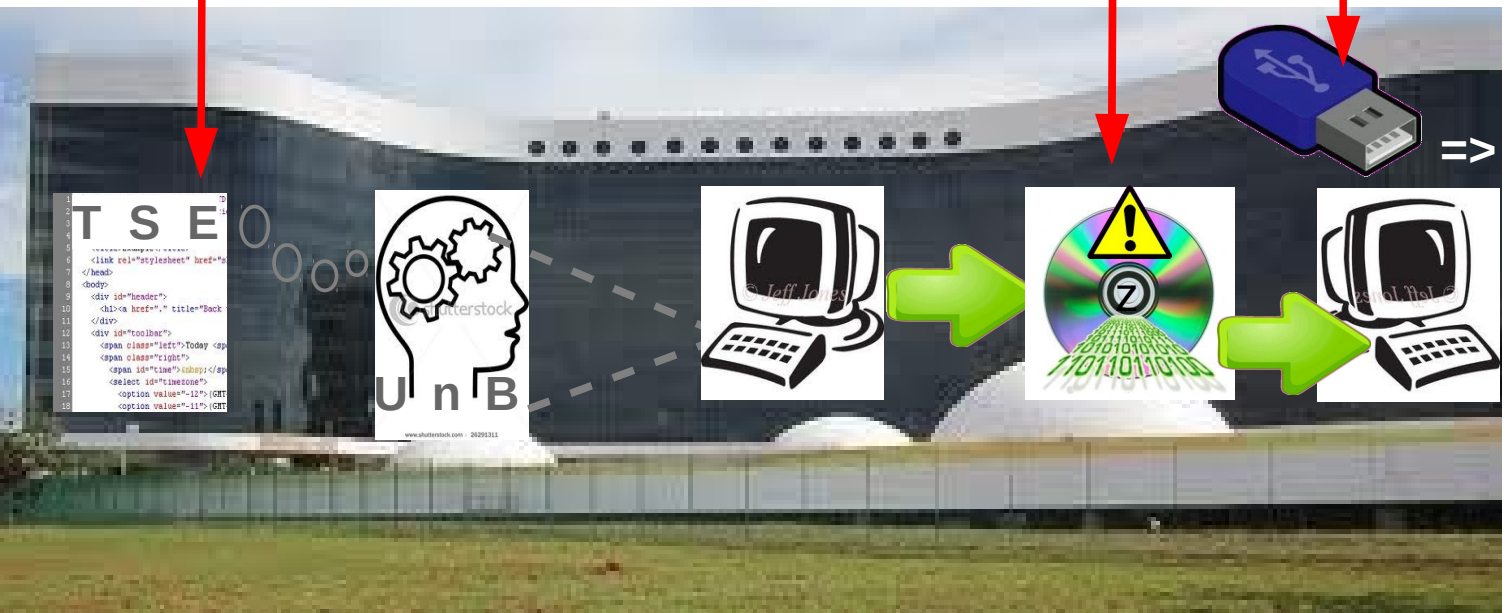

**RDV**s.

?

# Como decodificar? (3)

"*Foi dentro de um ambiente controlado. Isto ...*"

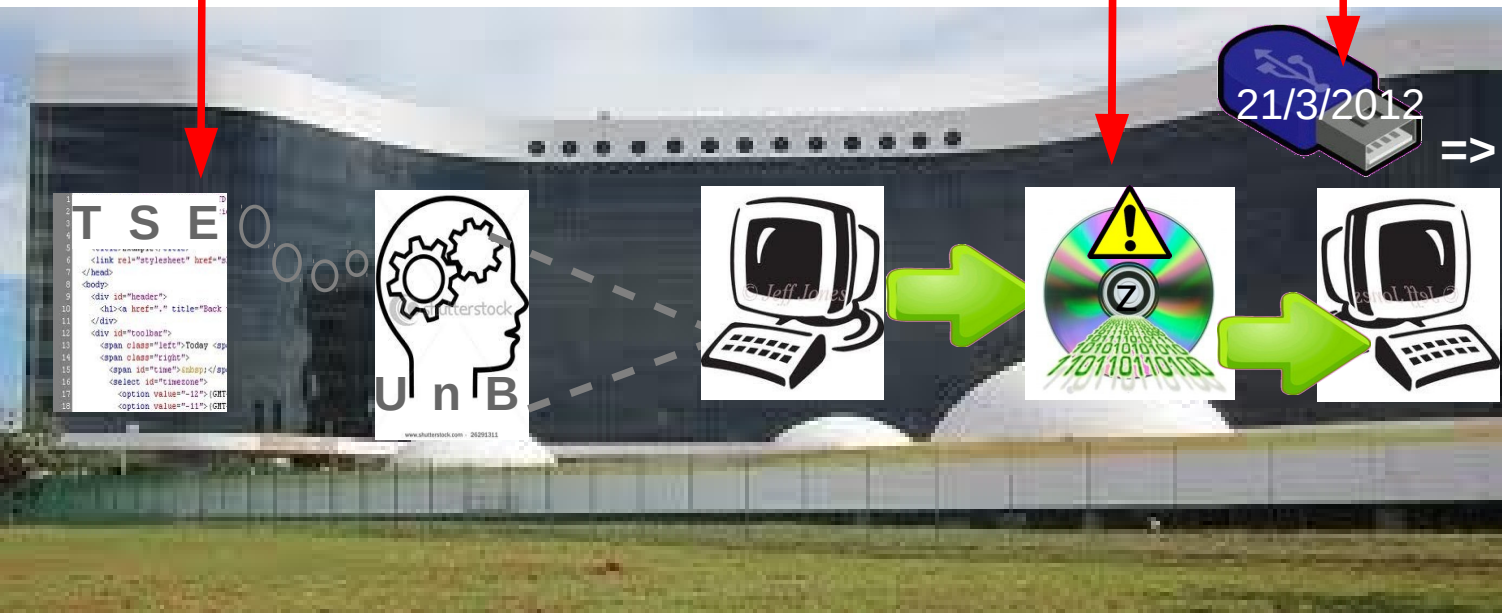
No ambiente controlado desses testes, “Isto” significa:
O código fonte desse software **revela** (a quem sabe),
como desembaralhar RDVs gerados por ele
em urnas de teste ...



# Como decodificar? (3)

"*Foi dentro de um ambiente controlado. Isto ...*"

No ambiente controlado desses testes, “Isto” significa:
O código fonte desse software **revela** (a quem sabe),
como desembaralhar RDVs gerados por ele
em urnas de teste. E *onde* mais?

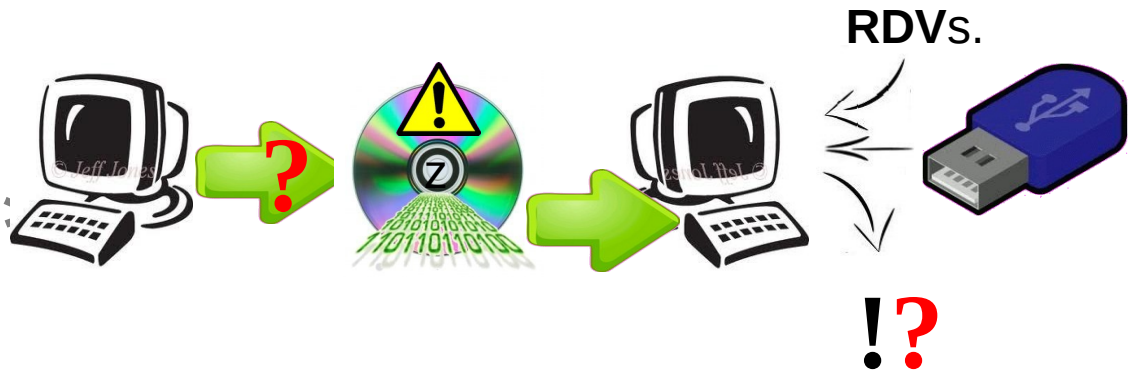


# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

Acesso a *qual* fonte?

Foto: Marcelo Ferreira
CB/D.A Press 20/3/12



# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.

À que seria das eleições 2008, 2010, muitos o tiveram

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.

À que seria das eleições 2008, 2010, muitos o tiveram

Como nas seguintes, terão, por direito a fiscalizar (lei)

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.
À que seria das eleições 2008, 2010, muitos o tiveram
Se a fonte de eleições passadas não tinham tal furo,
...

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.

À que seria das eleições 2008, 2010, muitos o tiveram

Se a fonte de eleições passadas não tinham tal furo, nem a das futuras terão


# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.
À que seria das eleições 2008, 2010, muitos o tiveram
Se a fonte de eleições passadas não tinham tal furo,
nem a das futuras terão, então, *pra que* esses testes?

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

A *qual* fonte? À do teste, **muitos** *já tiveram* acesso.
À que seria das eleições 2008, 2010, muitos o tiveram
Se a fonte de eleições passadas não tinham tal furo,
nem a das futuras terão, então, *pra que* esses testes?
Ou *é verdade* que a fonte era a mesma?

# Como decodificar? (4)

"*Isto numa situação real seria absolutamente impossível porque ele não teria acesso à fonte ...*"

Ou, *será verdade* que a fonte era a mesma?

Conforme o **Edital n° 01/2012** (que regulamenta a 2ª Edição dos "Testes de Segurança da Urna"):

*"os testes deverão considerar os seguintes elementos e componentes da urna: processo de carga; hardware;… ; conteúdo das mídias de dados;* ***software de votação utilizado na seção eleitoral."***

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir:

**RDV** e **Log** de uma seção Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

Semente

| | | | | | | |
|---|---|---|---|---|---|---|
| c | | | | | | |
| o | | | | | | |
| m | | | | | | |
| | | | | | | |
| L | | | | | | |
| o | | | | | | |
| g | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log** de uma seção Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

1º Voto

| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log** de uma seção Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

2º Voto

| | | | | | | |
|---|---|---|---|---|---|---|
| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
| **8:04 h** | pr | 23 | gv | 13 | se | 23 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log** de uma seção Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

3º Voto

| | | | | | | |
|---|---|---|---|---|---|---|
| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
| **8:04 h** | pr | 23 | gv | 13 | se | 23 |
| **8:15 h** | pr | 51 | gv | 13 | se | 15 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log** de uma seção Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

4º Voto

| | | | | | | |
|---|---|---|---|---|---|---|
| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
| **8:04 h** | pr | 23 | gv | 13 | se | 23 |
| **8:15 h** | pr | 51 | gv | 13 | se | 15 |
| **8:27 h** | pr | 23 | gv | 23 | se | 23 |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log**
de uma seção
Eleição 2010

Arquivos públicos a que todo partido político tem direito a acesso (L10.740)

5º Voto

| | | | | | | |
|---|---|---|---|---|---|---|
| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
| **8:04 h** | pr | 23 | gv | 13 | se | 23 |
| **8:15 h** | pr | 51 | gv | 13 | se | 15 |
| **8:27 h** | pr | 23 | gv | 23 | se | 23 |
| **9:02 h** | pr | 13 | gv | 15 | se | 51 |
| | | | | | | |
| | | | | | | |

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Em situações reais, *se* o Edital n° 01/2012 considera a si confiável, certos vínculos podem surgir (p. ex):

**RDV** e **Log**
de uma seção
Eleição 2010

Arquivos públicos
a que todo partido
político tem direito
a acesso (L10.740)

etc.

| | | | | | | |
|---|---|---|---|---|---|---|
| **8:01 h** | pr | 13 | gv | 51 | se | 15 |
| **8:04 h** | pr | 23 | gv | 13 | se | 23 |
| **8:15 h** | pr | 51 | gv | 13 | se | 15 |
| **8:27 h** | pr | 23 | gv | 23 | se | 23 |
| **9:02 h** | pr | 13 | gv | 15 | se | 51 |
| **...** | ... | ... | ... | ... | ... | ... |
| | | | | | | |

# Como decodificar? (5)

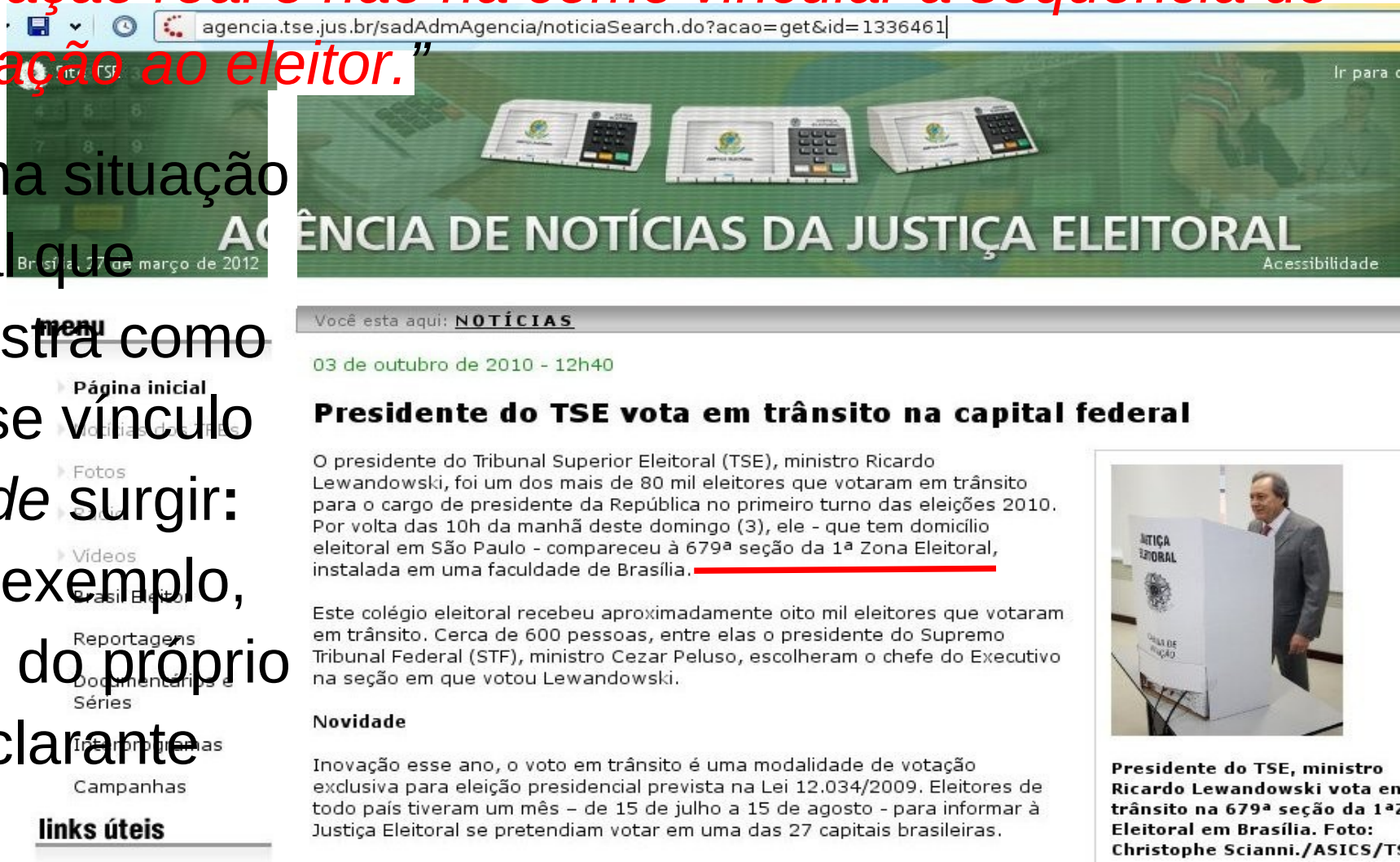
"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

Uma situação
real que
mostre como
esse vínculo
*pode* surgir?

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

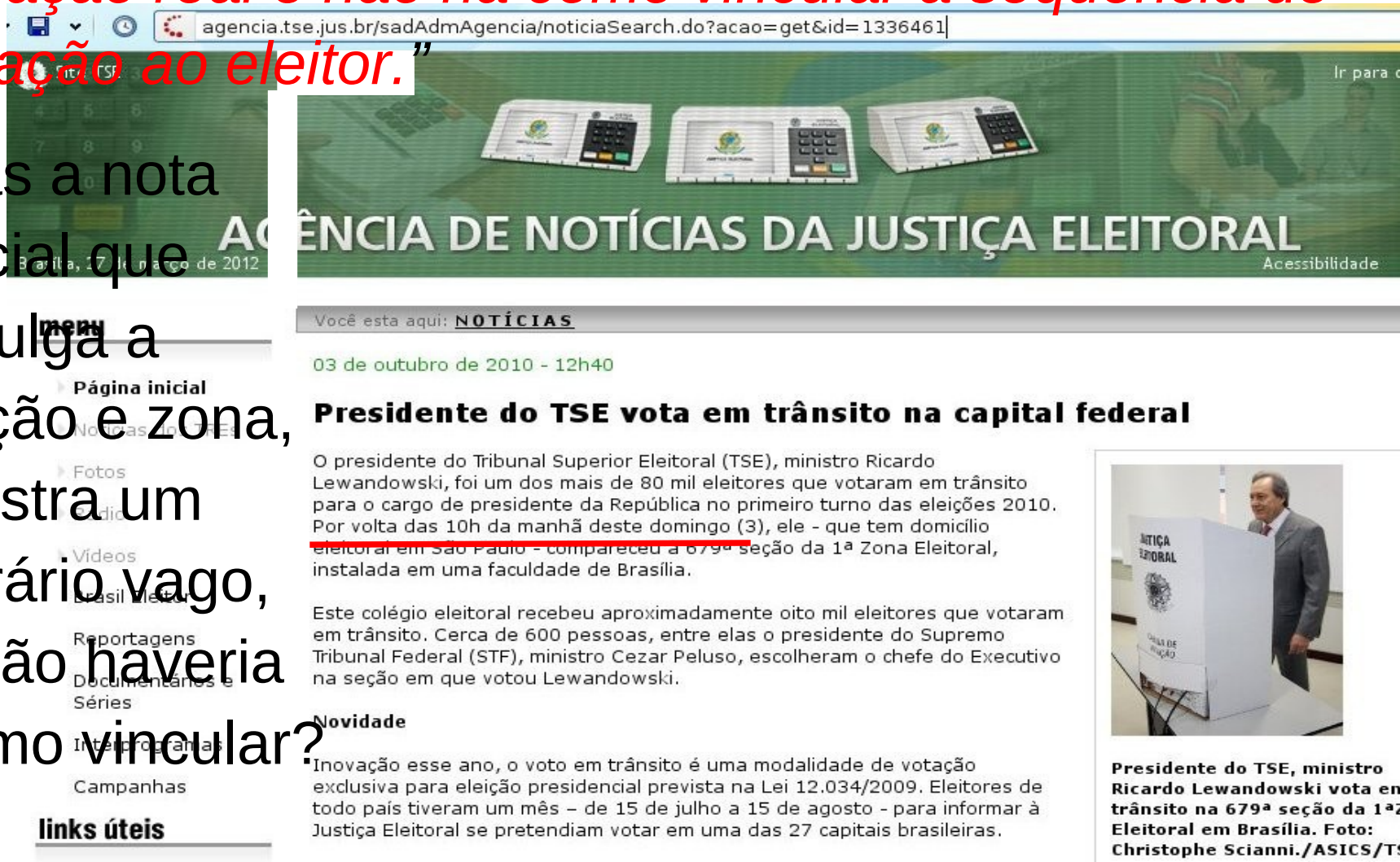
Uma situação real que mostra como esse vínculo *pode* surgir: no exemplo, um do próprio declarante



# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Mas a nota oficial que divulga a seção e zona, mostra um horário vago, e não haveria como vincular?



# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*"

Se a imprensa corporativa for crível em temas eleitorais, então o horário exato permite vincular, nesse exemplo do declarante.

www.correiobraziliense.com.br/app/noticia/especiais/eleicoes2010/2010/10/03/interna_eleicoes20

CORREIO BRAZILIENSE | ELEIÇÕES 2010

Brasília, domingo, 25 de Março de 2012

_eleicoes2010,216159/index.shtml

CAPA | BRASIL / ECONOMIA / POLÍTICA | CIDADES-DF | MUNDO | DIVERSÃO E ARTE | DIVIRTA-SE

CORREIO DIGITAL | SUPER ESPORTES | EU, ESTUDANTE | VÍDEO | ÁUDIO | GALERIA DE FOTOS | BLOGS

## Presidente do TSE, Ricardo Lewandowski, vota em trânsito no Iesb

Larissa Leite

Publicação: 03/10/2010 14:03 Atualização:

O presidente do Tribunal Superior Eleitoral, Ricardo Lewandowski, votou às 10h30 em seção eleitoral presente do Instituto de Educação Superior de Brasília (Iesb), que abrigou apenas justificativas e votos em trânsito (apenas para o cargo de presidente e vice-presidente da República). São esperados no local, até o final do dia de hoje, 8.132 eleitores. Lewandowski votou em trânsito, já que o seu título eleitoral é do estado de São Paulo.

O presidente do TSE chegou com meia hora de atraso e causou tumulto entre os presentes, pelo fato de não ter enfrentado fila para votação. "Eu estou trabalhando", justificou o ministro. No momento, outras pessoas também alegaram que estavam em horário de trabalho, mas não tinham prioridade por isto.

Irene Custódia de Jesus, 68 anos, era a primeira da fila no momento da chegada do presidente do TSE. "Foi uma confusão. Eu fiz uma cirurgia na cabeça e não posso cair. Só não me derrubaram por causa da ajuda de uma amiga", comentou. Lewandowski votou em apenas 1 minuto. Seguranças impediram a proximidade de algumas equipes de imprensa da sessão eleitoral, o que aumentou o transtorno no local.

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

*A quem* esta
situação real
permite, no exemplo,
vincular e identificar
o voto do declarante
na eleição de 2010?

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

A Resposta, por óbvio,
inclui todos *em posse do ou com acesso ao* RDV
e Log da 679ª Seção da
1ª Z.E. do DF de 2010,
e que tem/tiveram/terão
acesso ao respectivo código.

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

A Resposta, por óbvio, inclui todos *em posse do ou com acesso ao* RDV e Log da 679ª Seção da 1ª Z.E. do DF de 2010, e que tem/tiveram/terão acesso ao respectivo código. Pode incluir fiscais de partido, muitos no TREDF, seus terceirizados, etc.

# Como decodificar? (5)

"… *não é uma quebra, porque esta não era uma situação real e não há como vincular a sequência de votação ao eleitor.*”

Tal Resposta,
se não configura
quebra de sigilo
ou violação da urna,
configura ao menos
quebra de confiança de eleitores
que querem voto consciente e eleições limpas,
em algo/alguém responsável por nossas eleições.

# Processo de Votação

Porque numa eleição estão sempre envolvidos **interesses potencialmente conflitantes**:

- **Eleitores** (*via de regra*, que desejam lisura)
- **Candidatos a cargo** (*via de regra*, mais de um)
- **Administradores** do processo (Juízes eleitorais)
- **Técnicos** Internos (do TSE e TREs)
- **Auxiliares** Externos (fornecedores, terceirizados)
- **Mesários** (eleitores com função operativa)
- **Fiscais** (de partidos ou candidatos)

# Processo de Votação

**Interesses podem conflitar em vários pontos,** e não só em relação ao sigilo do voto:

- Tribunais (Regionais e Superior)
- Zonas / Comarcas Eleitorais
- Seções Eleitorais / Locais de Votação
- Locais de Armazenamento das Urnas
- Estações de Transmissão Digital (sw e dados)
- Meios de Disponiblização (sw, UEs, BUs, RDVs. Logs, tabelas de correspondência, resultados).

# “Segurança”

Conceito Técnico:

- **Segurança** = Controle da **proteção**

  *Proteger* **NÃO** é verbo intransitivo nem transitivo: é *bitransitivo*

- Protegese **ALGUÉM** (com algum interesse) **DE ALGO** (de um risco), e ***NÃO*** “A Urna/O Sistema”
- Mais de 2 interesses em jogo introduzem riscos de **CONLUIO**: Neste caso, segurança é **equilíbrio** de riscos e responsabilidades (sigilo x transparência)

# Segurança digital

Em processo (eletrônico) com mais de dois interesses em jogo, segurança **pressupõe:**

- Mapas de risco
- Auditorias independentes
- Fiscalização externa em pontos de conflito
- *Software* (todos) em código fonte auditável sem restrições (negociais, de compilação, de propriedade imaterial, etc.)
- Simulação de ataques (teste *realistas*)

# Não é só sigilo!

**Vulnerabilidades envolvendo participação externa, *mormente na totalização*, incluem**

- Voto de falecidos / ausentes (fraude cadastral)
- Transmissão de mídia clonada
- Clones a partir de *Flash* de Carga extraviados
- Vazamento da chave de assinatura da UE
- Código alterado ou ofuscado após fiscalização
- Extravio de BUs impressos (totalização)
- Quebra de sigilo por reordenação do RDV (Sandy)

# Não é só sigilo!

**Vulnerabilidades internas incluem:** (1)

**Brechas para inserção de cavalos de tróia**

- Para fraudes **por atacado** (num estado ou país):
  antes da compilação dos programas das UE
  antes da distribuição para TREs
- **Semi-atacado** (zonas): antes da carga das UE
- **De varejo** (sessões): depois da carga das UE
  via rootkit na BIOS (plugável e programável)
  via *flashcard* externo (novas UE, c/ chave vazada)
  via mídias de atualização das UE

# Não é só sigilo!

**Vulnerabilidades internas incluem:** (2)

**Brechas para ataques na totalização**

- Sonegação de BUs impressos na sessão eleitoral
  [art. 42 da Resolução TSE 22.154, maio de 2006]
  com troca do BU digital
  via urna inseminada por flash de carga clonado
  via falsificação do BU digital por chave vazada
  via alteração do Banco de Dados da totalização
- Sonegação do relatório de votos por sessão
  com alteração do Banco de Dados da totalização

# Não é só sigilo!

## Roteiro básico para cavalos de tróia na UE

- **Desarme** (imperceptível) da autoverificação de integridade (assiatura digital, hash etc.) no arquivo de controle de inicialização.
- Instalação de rotina para **desvio** de votos pós votação e prégravação do BU e RDV (baseado em porcentagens, limiares, etc.), em sw da UE
- **Autodeleção** (da rotina de desvio e do gatilho de desarme) após a gravação do BU e RDV.

# Como decodificar? (6)

"…*O eleitor pode ficar tranquilo que não é uma quebra…*”

Por que a reação
mais imediata
do eleitor comum
diante de críticas
ao nosso processo
como foi informatizado
tende a ser esta?

# Como decodificar? (6)

"…*O eleitor pode ficar tranquilo que não é uma quebra…*”

Por que a reação
mais imediata
do eleitor comum
diante de críticas
ao nosso processo
como foi informatizado
tende a ser *esta*?

# A seita do Santo Byte


Descrita em artigo sobre a estranha votação da Lei 10.740 (que tirou VVPT e introduziu RDV em 2003)

- No sacrário eletrônico (TV, etc.), adeptos ingerem uma beberagem marqueteira *pelos ouvidos*;
- Põemse a bailar com a grande mídia o mantra "*Nosso sistema é confiável, nunca ninguém provou o contrário, nós dominamos a tecnologia!*";
- Passam a ter visões, de seres angelicais programando urnas e apurando eleições. Vêem infiéis como retrógrados, paranóicos, impatriotas.

# Santo Byte, *circa* 1987

eJagube + eChacrona :

# Referências

**Evento onde esta palestra foi apresentada:**

http://ptbr.facebook.com/events/273721092692866

**Portal de publicações do autor:**

pedro.jmrezende.com.br/sd.php

**Comitê Multidisciplinar Independente:**

pt.everybodywiki.com/Comitê_Multidisciplinar_Independente

**Fórum do Voto Eletrônico:**

www.votoseguro.org