CCJC Câmara
8 mai 2012

Audiência Pública

PL 2789/11

Prof. Pedro A. D. Rezende

Ciência da Computação

Universidade de Brasília

O Sigilo do Voto

Cavalo de Batalha da Norma Eleitoral desde … a Revolução de 1930

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” – Lei 4737/65

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.
- Lei 9.504/97: Elimina registro material do voto em troca de transparencia do software da urna DRE.

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.
- Lei 9.504/97: Elimina registro material do voto em troca de transparencia do software da urna DRE.
- Lei 10.402/02: Reintroduz registro material, adaptando DREs em estoque para VVPTs, por ineficácia da troca.

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.
- Lei 9.504/97: Elimina registro material do voto em troca de transparencia do software da urna DRE.
- Lei 10.402/02: Reintroduz registro material, adaptando DREs em estoque para VVPTs, por ineficácia da troca.
- Lei 10.740/03: Anula adaptação a VVPTs, em troca de RDV para fins de auditoria externa do voto.

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.
- Lei 9.504/97: Elimina registro material do voto em troca de transparencia do software da urna DRE.
- Lei 10.402/02: Reintroduz registro material, adaptando DREs em estoque para VVPTs, por ineficácia da troca.
- Lei 10.740/03: Anula adaptação a VVPTs, em troca de RDV para fins de auditoria externa do voto.
- Lei 12.034/09: Rereintroduz registro material via VVPT por ineficácia do RDV como ferramenta fiscalizatória.

O Sigilo do Voto

Cavalo de Batalha desde… a Revolução de 30

- Lei 4.737/65: Exige embaralhamento dos votos que saem da urna, como garantia deste sigilo.
- Lei 9.504/97: Elimina registro material do voto em troca de transparencia do software da urna DRE.
- Lei 10.402/02: Reintroduz registro material, adaptando DREs em estoque para VVPTs, por ineficácia da troca.
- Lei 10.740/03: Anula adaptação a VVPTs, em troca de RDV para fins de auditoria externa do voto.
- Lei 12.034/09: Rereintroduz registro material via VVPT por ineficácia do RDV como ferramenta fiscalizatória.
- ADI 4543 suspende – e PL 2789/11 reanula – rereadaptação a VVPT, mantendo RDV.

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

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.”

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

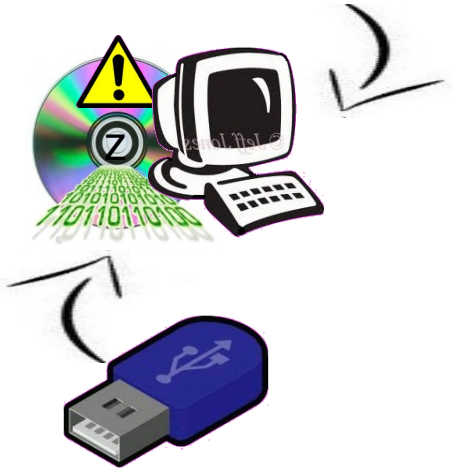
RDV, Log:

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		

1º Voto

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		

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? (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?

"… *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						

Desembaralhamento

"… *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

Desembaralhamento

"… *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

Desembaralhamento

"… *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

Desembaralhamento

"… *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

Desembaralhamento

"… *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?

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

Numa situação real E NORMAL, **a Norma Eleitoral (Leis 9.504/97, 10.720/03, etc.) deve ser cumprida pela autoridade executora do processo eleitoral:**

1 a fonte do código que embaralha votos DEVE SER a mesma que os fiscais de partido conheceram na cerimônia de compilação, e

2 os RDVs devem ser entregues aos fiscais que solicitarem.

Como decodificar?

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

Numa situação real E NORMAL, **a Norma Eleitoral (Leis 9.504/97, 10.720/03, etc.) deve ser cumprida pela autoridade executora do processo eleitoral.**

Uma eleição oficial é uma situação real e NORMAL?

Como decodificar?

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

Numa situação real E NORMAL, **a Norma Eleitoral (Leis 9.504/97, 10.720/03, etc.) deve ser cumprida pela autoridade executora do processo eleitoral.**

Uma eleição oficial é uma situação real e NORMAL?

Como decodificar?

"… *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 E NORMAL – **onde a Norma Eleitoral (Leis 9.504/97, 10.720/03, etc.) está sendo cumprida pela autoridade eleitoral** – a fonte do código que embaralha votos DEVE SER a mesma que os fiscais de partido conhecem.

Uma eleição oficial é uma situação real e NORMAL?

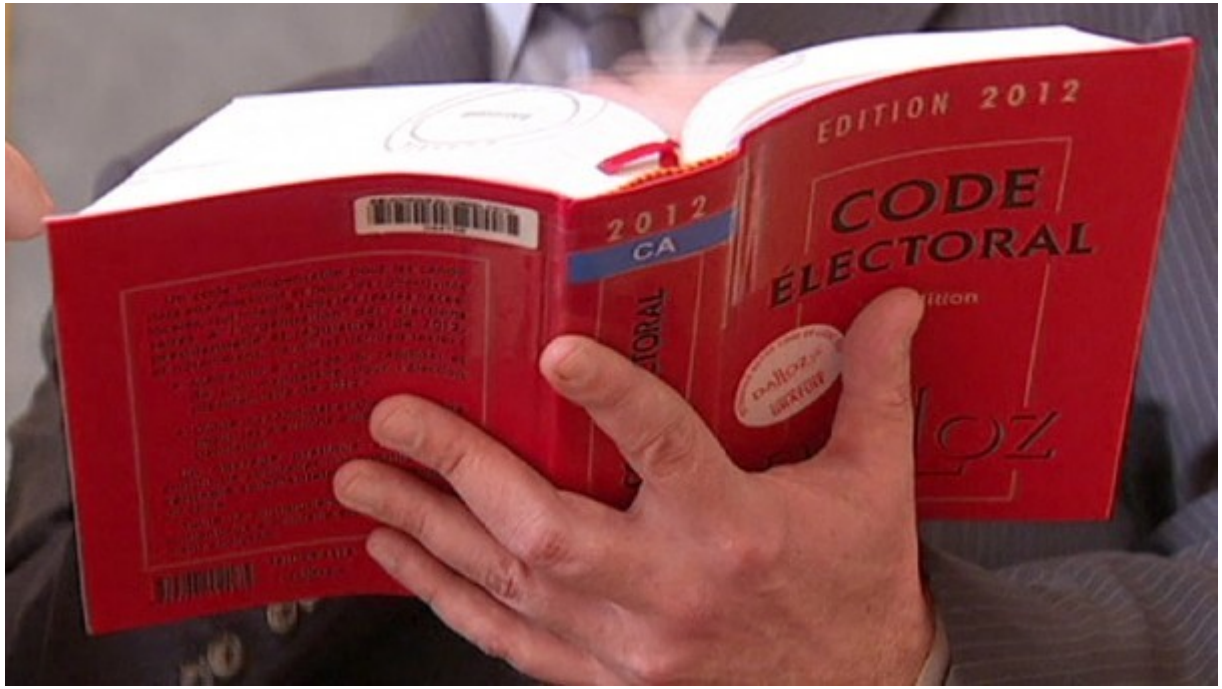
Como decodificar?

"… *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 E NORMAL – **onde a Norma Eleitoral (Leis 9.504/97, 10.720/03, etc.) está sendo cumprida pela autoridade eleitoral** – a fonte do código que embaralha votos DEVE SER a mesma que os fiscais de partido conhecem.

Uma eleição oficial é uma situação real e NORMAL?

Como tudo começou



Períodos da história

Períodos da história

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:

www.cic.unb.br/docentes/pedro/sd.php

Comitê Multidisciplinar Independente:

pt.wikipedia.org/wiki/CMIND

Fórum do Voto Eletrônico:

www.votoseguro.org

Referências

Evento onde parte desta palestra foi inicialmente 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