UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE EDUCAÇÃO E SAÚDE - CES
UNIDADE ACADÊMICA DE EDUCAÇÃO
CURSO DE GRADUAÇÃO EM LICENCIATURA DA MATEMÁTICA

ÉRICA BRAGA DE AGUIAR

CRIPTOGRAFIA:

Decifrando Mensagens Secretas no Sistema Penitenciário Brasileiro.

CUITÉ- PB

2022

ÉRICA BRAGA DE AGUIAR

CRIPTOGRAFIA:

Decifrando Mensagens Secretas no Sistema Penitenciário Brasileiro.

Trabalho de Conclusão do Curso, apresentado ao Curso de Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande-UFCG, em cumprimento às exigências para obtenção de título de Licenciatura da Matemática.

Orientador: Prof. Dr. Luciano Martins Barros.

CUITÉ- PB

2022

A282c Aguiar, Érica Braga de.

Criptografia: decifrando mensagens secretas no Sistema Penitenciário Brasileiro. / Érica Braga de Aguiar. - Cuité, 2022.

79 f.: il. color.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Universidade Federal de Campina Grande, Centro de Educação e Saúde, 2022.

"Orientação: Prof. Dr. Luciano Martins Barros".

Referências.

1. Criptografia. 2. Sistema Penitenciário Brasileiro. 3. Decodificação. 4. Organização criminosa. 5. Comunicação – criptografia – facção criminosa. 6. Brasil - presídios. I. Barros, Luciano Martins. II. Título.

CDU 003.26(043)

FICHA CATALOGRAFICA ELABORADA PELO BIBLIOTECARIO Msc Jesiel Ferreira Gomes - CRB-15/256

ÉRICA BRAGA DE AGUIAR

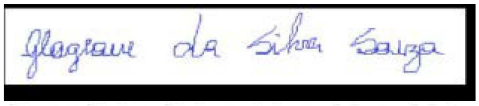
CRIPTOGRAFIA:

Decifrando Mensagens Secretas no Sistema Penitenciário Brasileiro.

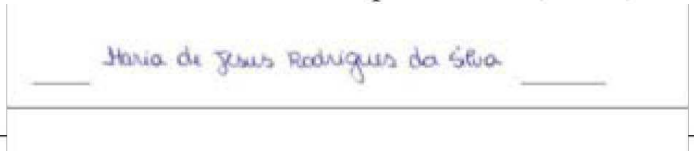
Trabalho de Conclusão de Curso apresentado à Banca Examinadora como exigência parcial à conclusão do Curso de Licenciatura em Matemática da Universidade do Federal de Campina Grande, UFCG, sob orientação do Prof. Dr. Luciano Martins Barros.

Aprovada em: ___/___/_____

Prof. Dr. Luciano Martins Barros
Universidade Federal de Campina Grande (UFCG)



Prof. Dra. Glageane da Silva Souza
Universidade Federal de Campina Grande (UFCG)



Prof. Msc. Maria de Jesus Rodrigues da Silva
Universidade Federal de Campina Grande (UFCG)

DEDICATÓRIA

Dedico este trabalho a Deus, a minha família e amigos que contribuíram muito na minha caminhada. Sem vocês eu nada seria.

AGRADECIMENTOS

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo da minha vida, e não somente nestes anos como universitária, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

Ao meu esposo Jurandir pelas vezes que cuidou de nosso filho Luiz Henrique, e de Helena, para que eu pudesse estudar e por compreender a minha ausência em muitos momentos.

À minha mãe Auriana e meus filhos: Heitor e Helena, agradeço pelo apoio.

A todos os meus familiares e amigos pelo incentivo neste momento tão importante da minha vida.

Ao Prof. Dr. Luciano Martins Barros pela orientação, apoio e confiança.

Aos professores que me acompanharam ao longo do curso, e que com empenho se dedicam a arte de ensinar.

A todos que direta ou indiretamente fizeram parte de minha formação.

RESUMO

A cada dia as organizações criminosas estão mais expressivas no país, e os membros dessas facções criminosas tendem a se comunicar, todavia, os criminosos sabem que a qualquer momento seus meios de comunicação possam ser interceptados pela justiça, utilizando então da criptografia para tentar dificultar qualquer investigação que venha a ter, muitas das vezes, essas comunicações ocorrem de informações saídas de dentro de presídios, logo o objetivo geral desta pesquisa é verificar até que ponto a matemática pode auxiliar na decodificação das mensagens secretas, que se tornaram comuns no dia a dia do sistema penitenciário brasileiro. A pesquisa tem uma abordagem qualitativa, utilizando como instrumento de coleta de dados um questionário online aplicado aos funcionários de presídios brasileiros, tendo como alvo mostrar a importância da desarticulação das ações criminosas que partem de dentro dos presídios do Brasil com o auxílio da matemática para decifrar as mensagens secretas entre as comunicações dos membros criminosos.

Palavras-chave: Criptografia; Organizações Criminosas; Sistema Penitenciário Brasileiro; Decodificação; Matemática.

ABSTRACT

Every day criminal organizations are more expressive in the country, and the members of these criminal factions tend to communicate, however, criminals know that at any time their means of communication can be intercepted by the justice, then using encryption to try to hamper any investigation that may have, many times, these communications occur from information coming out of prisons, so the general objective of this research is to verify to what extent mathematics can help in the decoding of secret messages, that have become common in the daily life of the Brazilian penitentiary system. The research has a qualitative approach, using as an instrument of data collection an online questionnaire applied to employees of Brazilian prisons, aiming to show the importance of dismantling criminal actions that come from within prisons in Brazil with the help of mathematics to decipher the secret messages between the communications of criminal members.

Keywords: Encryption; Criminal Organizations; Brazilian Penitentiary System; Decoding; Math.

"Educação não transforma o mundo,
Educação muda as pessoas.
Pessoas mudam o mundo".

(Paulo Freire)

SUMÁRIO

INTRODUÇÃO

Conceitualmente, a criptografia pega um texto simples, como uma mensagem de texto ou e-mail, e o embaralha em um formato ilegível – chamado "texto cifrado". Isso ajuda a proteger a confidencialidade dos dados digitais armazenados em sistemas de computador ou transmitidos por meio de uma rede como a Internet (OLIVEIRA, 2019). Nesse sentido, ao passo que se trata de ferramenta útil para cumprir com os objetivos efêmeros da informação e também da segurança da informação no período, também pode ser utilizada para reduzir a eficácia e a qualidade da segurança pública, em que pese proporcionar um ambiente de maior segurança à luz do crime organizado.

Ao embaralhar o texto legível para que possa ser lido apenas pela pessoa que possui o código secreto ou a chave de descriptografia, a criptografia ajuda a fornecer segurança de dados para informações confidenciais, sejam elas tuteladas sobre o direito ou baseadas em operações criminosas e suas organizações. Grandes quantidades de informações pessoais são gerenciadas online e armazenadas na nuvem ou em servidores com conexão contínua à web. É quase impossível fazer qualquer negociação sem que seus dados pessoais acabem entrando no sistema de computadores, e é por isso que é importante saber como ajudar a manter esses dados privados. Assim, a criptografia desempenha um papel essencial nessa tarefa (SOUSA, 2009) e, ao mesmo tempo, desempenha aporte tecnológico importante para que toda a transferência de informação ocorra de forma sigilosa quando se trata de ações que fogem à luz da lei, isto é, que são criminosas.

Nesse sentido, muito embora os benefícios e desafios desta tecnologia contemporânea sejam observáveis à sociedade e à ciência, poucos são os estudos que buscam avaliar toda a sua reprodução no sistema penitenciário, mesmo ocorrendo de cada dia ser mais comum nos noticiários jornalísticos as ordens criminosas saindo de dentro dos presídios determinadas pelos líderes das organizações criminosas encarcerados, o que implicou no desenvolvimento deste projeto que visa, sobretudo, estabelecer, por meio de uma pesquisa qualitativa, as utilizações da Criptografia no dia-a-dia da penitenciária brasileira, elencando os desafios, os meios de comunicação e o atual estado de combater os problemas da polícia brasileira. A este objetivo, busca-se, em específico, avaliar a história da Criptografia, os componentes contemporâneos e seus usos bem como todas as classificações do sistema prisional brasileiro.

Frente a isto, esta pesquisa se divide em quatro capítulos centrais. O primeiro traz a caracterização histórica da Criptografia. O segundo apresenta seu aporte contemporâneo e as suas ferramentas atuais. Já o terceiro elenca o sistema prisional brasileiro e suas características. Por fim, tem-se um capítulo que apresenta um estudo aplicado desenhado em penitenciárias brasileiras, a partir da perspectiva dos funcionários.

Capítulo I
História da Criptografia

Neste primeiro capítulo, abordaremos a História da Criptografia, desde os seus primeiros vestígios na Antiguidade, seguido dos seus avanços ao longo dos anos, destacando os seus principais ápices até a atualidade.

1.1 A Criptografia

O problema da troca de informações privadas, indecifráveis por terceiros, está mais atual do que nunca. Se durante séculos a criptografia esteve associada aos aspectos demasiados distantes da vida cotidiana e até algumas décadas atrás era usada, sobretudo, no campo militar e governamental, hoje, especialmente, os indivíduos tendem a utilizá-la diariamente, mesmo que muitas vezes inconscientemente (LUND, 2019).

A tecnologia da informação e a Internet tornaram o problema do sigilo da comunicação cada vez mais relevante. Ações que se realizam todos os dias, como ligar pelo celular, abrir o carro com o controle remoto ou utilizar um caixa eletrônico, significam transmissão de informações que podem ser capturadas e exploradas em detrimento das ações humanas. Para evitar que isso aconteça, é necessário garantir que, mesmo que uma terceira pessoa em potencial intercepte a mensagem, ela pareça incompreensível para ele. O próprio destinatário terá, portanto, a certeza não apenas de que as informações permaneceram secretas, mas também de que as informações não foram adulteradas por terceiros (ARAÚJO, 2018).

A criptografia trata justamente do conjunto de sistemas capazes de tornar uma mensagem incompreensível para qualquer pessoa que a possua, com exceção do destinatário legítimo. A criptoanálise, por outro lado, é a arte de forçar tais sistemas. Numerosos matemáticos em diferentes períodos históricos tentaram sua mão em criptoanálise; por exemplo, o caso da violação da criptografia da máquina Enigma, o sistema criptográfico utilizado pelo exército nazista durante a Segunda Guerra Mundial, principalmente devido ao matemático polonês Marian Rejewski e depois completado por um grupo de cientistas ingleses, entre os quais o famoso lógico Alan Turing que desempenhou um papel de destaque, entre muitos outros. Nesse sentido, a matemática implicou em competências importantes ao longo das ações e envolvimento dos homens, historicamente e nos dias atuais (ARAÚJO, 2018).

Hoje, a matemática é vital no desenvolvimento da criptografia e da criptoanálise, fator que se deve especialmente após a década de 1970 com a introdução da criptografia de chave pública e outros protocolos semelhantes. A necessidade de trocar informações secretas, no entanto, não diz respeito apenas aos tempos mais recentes, mas também ao passado. De fato, acredita-se que a criptografia seja tão antiga quanto a escrita e já na Bíblia três tipos diferentes de cifras são usados para ocultar algumas palavras específicas: o Código Atbash (que será analisado neste capítulo), o Código Albam e o Código Atbah. O exemplo mais antigo de criptografia consiste em um bastão no qual uma pequena tira de couro ou papiro, era enrolada nesta vara de madeira ficando conhecido como foice de Lacedemônio, ou ainda, Bastão de Licurgo, com uso por volta de 400 a.C, (BARCZAK, 2014).

Compreendida sua importância, este capítulo objetiva reconstituir as etapas mais importantes da história da criptografia desde a antiguidade até os dias atuais, relacionando as novas técnicas com teorias matemáticas subjacentes a elas. Suas seções expõem o desenvolvimento de sistemas criptográficos a partir do século 4 a.C, passando às novas técnicas utilizadas durante a Primeira Guerra Mundial, repassando o papel de destaque que a criptografia desempenhou durante a Segunda Guerra Mundial e, em particular, sobre a importância de descriptografar mensagens criptografadas pelos alemães usando a máquina Enigma, que foi um passo, de fato, com grande importância para popularizar este modelo de transmissão de informação (SANTOS, 2014; BARCZAK, 2014).

Expondo esta importância, expõem-se também os métodos modernos de criptografia, procurando as relações que existem hoje entre criptografia, matemática e ciência da computação. Considera-se, sobretudo, a história moderna do ocidente, por sua implicação diretiva no desenvolvimento do Brasil, em que a criptografia é diretamente dependente em resultado. Tem-se, portanto, o foco em trazer a criptografia como disciplina em contínua evolução e na qual a matemática (álgebra e teoria dos números em particular) desempenha um papel de primordial importância, como uma ferramenta cada vez mais necessária à medida que o desenvolvimento de novos sistemas de criptografia progride. Os dados aqui colhidos devem ser discutidos a partir dos resultados da pesquisa prática, também.

O termo *criptografia* vem do grego *kryptos* que significa *escondido* e *graphía*, que significa *escrita*. A criptografia é, portanto, a arte de escrever mensagens secretas. Refere-se a um conjunto de métodos, técnicas e algoritmos que tornam possível transformar uma

mensagem de forma a torná-la inteligível apenas para pessoas que compartilham mais informações sobre o método pelo qual a mensagem foi codificada (PRIETO, 2020).

Supõe-se, por exemplo, que duas pessoas queiram trocar remotamente informações que devem permanecer confidenciais: a mensagem trocada não deve, logo, ser acessível a terceiros. Quando isso ocorrer, diz-se que o canal de transmissão é seguro, embora, na realidade, nenhum canal pode ser considerado verdadeiramente seguro (PRIETO, 2020). O remetente deve tentar manter a confidencialidade *ocultando* informações contidas na mensagem e para isso utiliza um sistema de criptografia que transforma o texto simples em um criptograma (texto cibernético), aparentemente sem sentido e de tal forma que somente o destinatário legítimo poderá extrair a informação transmitida (WALLACE, 2019). Se o canal de transmissão não for seguro, terceira pessoa (oponente) pode tentar interceptar a mensagem e descriptografá-la (papel passivo) ou, mesmo, para intrometer suas mensagens no canal (papel ativo). O sistema funciona se e somente se o remetente e o destinatário compartilharem um segredo, do qual o oponente não deve estar ciente, sendo este segredo a chave do sistema que pode utilizar diversificadas ferramentas para se formar, tal como a matemática (WALLACE, 2019).

1.2 Criptografia Antiga

Desde os tempos antigos, o homem sentiu a necessidade de transmitir mensagens secretas; de fato, os primeiros exemplos de criptografia foram descobertos em alguns hieróglifos egípcios que datam de mais de 4.500 anos atrás (COSTA, 2014). Nos escritos minuciosos de Plutarco (filósofo grego platônico médio), aprende-se sobre o uso da escrita lacedemônio por volta de 400 a.C: um sistema criptográfico rudimentar que foi explorado pelos espartanos, especialmente em tempos de guerra, para comunicações curtas. A foice era uma pequena vara de madeira, a mensagem estava escrita em um pequeno pedaço de couro ou papiro enrolado em volta dela. A Figura 1 apresenta sua estrutura.

Figura 1: Sistema Criptográfico Rudimentar de Esparta

Fonte: Retirado de Museu Informática (2021)

Uma vez que a tira de pele foi desenrolada da foice, era impossível decifrar a mensagem. A chave do sistema consistia no diâmetro da foice, a decriptação só era possível se estivesse de posse de uma varinha idêntica à do remetente, portanto é um sistema criptográfico com chave simétrica (este é um sistema criptográfico que usa a mesma chave para criptografia e descriptografia. (WALLACE, 2014; COSTA, 2019). Em frente, avalia-se um dos mais famosos códigos da história antiga: o Código Atbash.

Quanto ao código Atbash, numerosos exemplos de escrituras secretas também podem ser encontrados em textos sagrados, muitas vezes usados para atacar a cultura dominante ou as autoridades políticas. Vários tipos de códigos cifrados foram encontrados no Antigo Testamento, incluindo o Código Atbash, usado no livro de Jeremias para criptografar o nome da cidade de Babilônia. A cifra Atbash é exemplo de código monoalfabético muito simples e consiste em substituir a primeira letra do alfabeto hebraico (alef) pela última (taw), a segunda (beth) pela penúltima (shin) ... e assim por diante (WALLACE, 2014; COSTA, 2019; PAPANI; SILVA, 2021; ARAÚJO, 2018).

Em sistemas criptográficos monoalfabéticos, as mesmas letras da mensagem clara são criptografadas com as mesmas letras no criptograma. O esquema geral de criptografia-descriptografia de um código monoalfabético é, portanto, representado por uma matriz quadrada *NxN,* com *N* = número de letras do alfabeto considerado. A chave do sistema é a própria mesa de correspondência e, por ser de difícil memorização, deve ser guardada em papel, com maior risco de furto.

O Código César e o Código Atbash são exemplos de códigos monoalfabéticos muito simples. Uma implementação interessante é a do Código monoalfabético, em que

as funções de criptografia e descriptografia são compostas por transformações lineares (WALLACE, 2014; COSTA, 2019; PAPANI; SILVA, 2021; ARAÚJO, 2018).

Neste código a chave (sempre simétrica) é composta por um par de inteiros: $K = (f, t)$ com: $0 < f < 26$: fator de multiplicação invertível *módulo 26;* $0 \leq t < 26$. Isso significa que f deve ser relativamente primo em relação a 26. Então existem 12 escolhas possíveis para *f:* $f \in 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.$ A função de criptografia é escrita: $c = E(m, K) = (m * f + t) \bmod 26$. O de decifrar: $m = [f^{-1}(c - t)] \bmod 26$ (WALLACE, 2014; COSTA, 2019; PAPANI; SILVA, 2021; ARAÚJO, 2018).

Ao atacar um código monoalfabético, decifrar uma única mensagem significa basicamente ter a chave do sistema em mãos e, portanto, também ter a possibilidade, para o oponente, de desempenhar um papel ativo ao inserir mensagens enganosas no canal. Um código César, por exemplo, é muito fácil de violar pois o espaço das chaves é muito pequeno enquanto o código monoalfabético afim (transformação linear) é um pouco mais resistente já que o espaço das chaves tem ordem $12x26 - 1 = 311$ (*12 possíveis f, 26 t possíveis, menos a cifra trivial* $f = 1, t = 0$). Finalmente, o espaço das chaves de um sistema monoalfabético generalizado (permutação) tem ordem 26! (cerca de $4x1026$ o que tornará um ataque de força bruta impraticável) (WALLACE, 2014). Aplicando-o ao alfabeto brasileiro, obtém-se:

Texto simples	*A B C D ... W X Y Z*	*(A1)*
Criptograma	*Z Y X W ... D C B A*	*(A2)*

O uso da criptografia nos escritos religiosos dos primeiros cristãos só terminou com o advento do imperador Constantino I, que se converteu ao cristianismo. Tão logo, já no Século 2 d.C., outro código surgiu, conhecido como: sistema criptográfico, em uso até o Renascimento, sendo o código simétrico mais simples possível: este era o chamado Código de César.

Nesse sentido, considere-se o alfabeto latino de 26 caracteres e, à sua memorização, defina-se para esta uma escala de números de 0 a 25. Nesse caso, define-se um número de 0 a 25 que será a chave secreta K. A operação de criptografia usando o Código de César consiste em adicionar K a cada caractere da mensagem de texto simples: o criptograma, ou seja, é obtido movendo-se para frente de K coloca cada caractere da mensagem de texto simples.

Graças ao testemunho de Suetonius, sabe-se que César usou K = 3 como chave de criptografia (COSTA; FIGUEIREDO, 2010; LUND, 2019; ENCINAS, 2016), tal como:

Texto simples	"JÚLIO CÉSAR"	(B1)
Chave Secreta	m = "JÚLIO CÉSAR	(B2)
Criptograma	c = m + 3 = "MXOLXVFDHVDU	(B3)

Essa string constituía, portanto, a mensagem confiada ao mensageiro e, teoricamente, mesmo que tivesse caído em mãos inimigas, a confidencialidade permanecia garantida pelo fato de o inimigo não conhecer a tecla K. Apenas o destinatário legítimo, que conhecia a chave, poderia recuperar a mensagem original do criptograma, mas realizando a operação inversa, ou seja, mas *voltando* por K lugares, movendo cada letra do criptograma (COSTA; FIGUEIREDO, 2010; LUND, 2019).

Para a criptografia, segundo o Código de César, deve-se imaginar o alfabeto escrito em uma coroa circular (... XYZABC ...) sem solução de continuidade. Por exemplo, sejam a, b dois inteiros e num inteiro positivo chamado módulo. A definição a e b são módulos congruentes n ($a \equiv b \pmod{n}$) *se n divide (a - b),* ou seja, se a divisão por n de a e b der o mesmo resto. (COSTA; FIGUEIREDO, 2010; LUND, 2019).

Uma vez que um módulo *n* foi definido, a classe de equivalência módulo *n* é o conjunto de todos os inteiros que têm o mesmo resto em relação ao divisor *n*. O conjunto de classes de equivalência cria uma partição do conjunto de inteiros. Pode-se, portanto, falar de operações de adição e multiplicação entre esses novos objetos matemáticos avaliados (COSTA; FIGUEIREDO, 2010; LUND, 2019; ENCINAS, 2016).

Matematicamente, a cifra de César é uma operação de adição de módulo 26 e a descriptografia é uma operação de diferença de módulo 26. Se o oponente conseguir pegar o criptograma e suspeitar que é um Código de César, pode tentar um ataque de força bruta (busca exaustiva no espaço das chaves), tentando descriptografar a mensagem com todas as chaves possíveis de K = 1 (para K = 0 existe uma criptografia trivial que deixa a mensagem inalterada) até K = 25, esperando encontrar uma mensagem de sentido completo.

Este tipo elementar de ataque é possível pelo número extremamente pequeno de chaves: o Código de César garante, portanto, segurança ruim, ao contrário da época de César, em esse tipo de sistema criptográfico era bastante seguro, considerando que muitas vezes os inimigos não conseguiam nem ler um texto simples, muito menos nunca um

criptografado e, além disso, não havia métodos de criptoanálise capazes de quebrar esse código, por mais trivial que fosse (LUND, 2019; ENCINAS, 2016).

Todavia, além desses dois códigos, também outros foram importantes nesta época, como Polybios. É nomeado assim, graças a um escritor grego (Grécia, 200 a.C – 118 a.C), que tinha o mesmo nome. Seu método consistia em colocar as letras do alfabeto em uma rede quadrada de $5x5$, a criptografia era baseada na correspondência de cada letra do alfabeto a um par de letras que indicava a linha e a coluna. A Figura 2 apresenta a sua estrutura:

Figura 2: Criptografia de Polybios em Letras

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I, J	K
C	L	M	N, Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Fonte: Elaborado pela Autora (2022)

Veja-se, em frente, um exemplo sobre o construto "DESEJAMOS PAZ". Este se tornaria ADAEDCAEBDAACBCDDC CEAAEE. Ao inserir números no quadro Polybios, considerando as linhas e colunas enumeradas de 1 a 5 obtém-se a criptografia em números Polybios.

Desta forma, cada letra é representada por dois números, pelo da sua linha e pelo da sua coluna. Então, $H = (2, 3)$; enquanto que no caso de N e Ñ têm a mesma numeração, sendo: $N = (3.3)$, Ñ = (3.3). Aplicando o exposto, na mesma mensagem "DESEJAMOS PAZ" é transformada na seguinte codificação numérica: 141543152411323443 351155.

Posto isto, é importante mencionar que, no caso da cifra de César e o método Polybios, estes são exemplos de substituição, o que significa que cada letra da mensagem original tem uma correspondência fixa com a mensagem criptografada. Por outro lado, o Bastão de Licurgo ou cítala espartana é um exemplo claro de transposição, ou seja, as letras são simplesmente trocadas de posição ou transpostas, de modo que as letras se tornam as mesmas tanto no texto original quanto no criptografado. O Código Atbash também é método de substituição. Em frente, trata-se da criptografia medieval e renascentista.

1.3 Criptografia Medieval e Renascentista

Até o ano 1.000, a criptografia era usada quase exclusivamente para ocultar nomes próprios em manuscritos; muitas vezes para fazer isso cada letra do alfabeto era simplesmente trocada com a próxima, criptografando assim seguindo o método de César com a chave 1. Por volta do século IX, ocorre uma das maiores descobertas da criptoanálise que permitiu violar mais facilmente os códigos de substituição monoalfabética usados até aquele período (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021).

De fato, o matemático e filósofo árabe, Al-Kindi é creditado com o desenvolvimento de um novo método segundo o qual a frequência da ocorrência de letras pode ser analisada e usada para quebrar um código (criptoanálise para análise de frequência). (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010). Os códigos monoalfabéticos têm uma falha séria: o mesmo caractere da mensagem de texto simples é sempre criptografado da mesma maneira. Em cada idioma é possível estudar a frequência com que determinado caractere ocorre em um texto, por exemplo, em italiano as letras "a" e "e" são as mais frequentes e, portanto, em criptograma, as cifras correspondentes aparecerão com a mesma frequência.

A análise de frequência, portanto, representa o *picklock* eficaz para violar um código monoalfabético, desde que se possua um texto cifrado longo o suficiente (PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010). Da necessidade de encontrar novos métodos que não sejam vulneráveis à análise de frequência, nascem as cifras polialfabéticas. Estas diferem das monoalfabéticas, pois um determinado caractere do texto claro nem sempre é criptografado com o mesmo caractere, mas com caracteres diferentes com base em alguma regra, geralmente vinculada a uma palavra secreta a ser acordada. Pode-se observar as primeiras cifras polialfabéticas no "Manuscrito para Decifrar Mensagens Criptografadas" escrito por Al-Kindi por volta de 800 d.C., mas o verdadeiro pai das cifras polialfabéticas é considerado Leon Battista Alberti (WAZLAWICK, 2016).

Até o final do século XIV, as cifras monoalfabéticas eram usadas quase que exclusivamente, todas as quais podiam ser violadas através da análise de frequência. Como consequência, nos três séculos seguintes, o código de Leon Battista Alberti formou a base dos sistemas criptográficos na busca de trazer segurança aos modelos existentes

(WAZLAWICK, 2016). Nesse caso, na Europa, a criptografia assumiu uma importância considerável como consequência da competição política e da revolução religiosa.

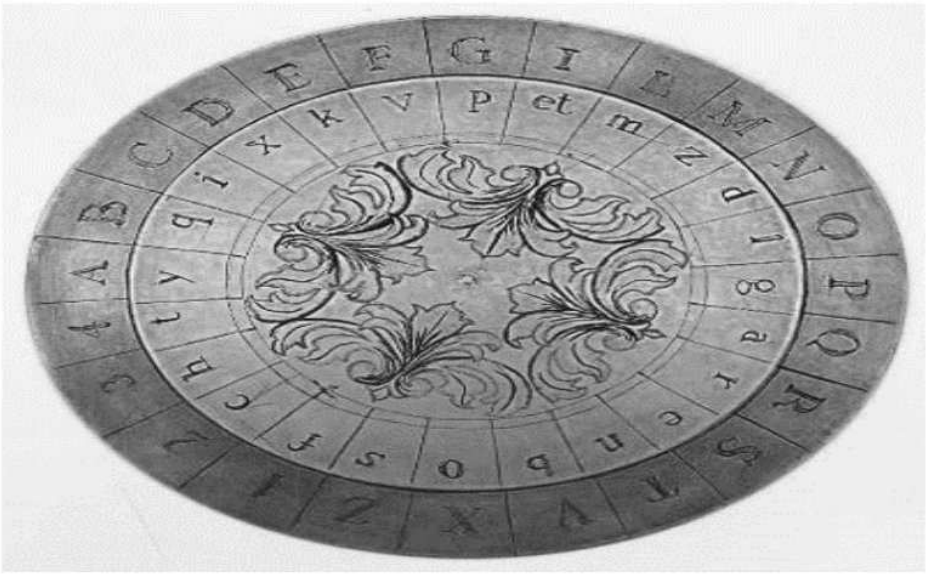
Durante e após o período do Renascimento, diversificados matemáticos e estudiosos de diferentes estados deram origem a uma rápida proliferação de técnicas criptográficas, algumas das quais refletiam o conhecimento dos estudos de Alberti sobre técnicas básicas de substituição polialfabética (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010).

Em 1586, o diplomata e criptógrafo francês Blaise de Vigenère publicou uma das cifras polialfabéticas mais simples, considerada inatacável por séculos. A Cifra de Vigenére tinha como ponto forte o uso não de um, mas de 26 alfabetos para criptografar uma única mensagem, seguindo um método que pode ser considerado uma generalização do código de César. De tal método deriva a Cifra de Vernam (BARCZAK, 2014), considerada teoricamente perfeita (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010), abordada em momento oportuno.

Por volta de 1467, Leon Battista Alberti descreve em seu tratado “De cifris” um novo método de criptografia polialfabética que representará um verdadeiro ponto de virada na história da criptografia ocidental. O novo método requer um dispositivo mecânico, chamado de disco de cifra. Este último é composto por dois discos de cobre concêntricos (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010).

O disco principal (disco estável) é dividido em 24 partes iguais, também chamadas de Case. As letras do alfabeto em texto simples são então mostradas sobre elas: 20 letras em ordem alfabética, excluindo as letras "inúteis" (H, K, Y, W) e considerando J = I e V = U e os números de 1 a 4. Nas casas do círculo interno (disco móvel), por outro lado, todas as 24 letras do alfabeto são mostradas (considerando apenas I = J e U = V), mas sem ordem particular e um símbolo especial final (ou " et) (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010). A Figura 3 apresenta a estrutura do disco de Alberti.

Figura 3: Disco de Leon Battista Alberti



Fonte: Adaptado de Museu del Calcolo (2022)

O remetente e o destinatário devem ter o mesmo disco e ter acordado uma chave de criptografia, composta por um par de letras que determinam a correspondência inicial entre os caracteres dos dois discos. Para criptografar a mensagem, o remetente escreve a mensagem em texto simples, sem espaços e inserindo aleatoriamente números de 1 a 4 dentro do texto. Portanto, a cada letra da mensagem de texto simples, que deve ser lida no disco maior, associa a letra correspondente no disco menor.

Isso acontece até que um dos números seja encontrado: nesse ponto, a letra correspondente ao número determina uma nova disposição: a letra A (a primeira letra da chave) é correspondida pela deduzida do número. O disco de Alberti é considerado uma das cifras polialfabéticas mais seguras, que não obteve o sucesso merecido também por decisão do próprio criador (seu tratado foi publicado em Veneza apenas um século após, passou quase despercebido) (WAZLAWICK, 2016; BARCZAK, 2014; PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010). Em frente, avalia-se o Código ou Cifra de Vigenère.

No final do século XVI, Vigenère propôs um novo método de codificação de chave polialfabética e simétrica. Este método foi baseado na idealização de que a fragilidade do código monoalfabético pode ser superada tornando a criptografia de um caractere dependente da posição que o caractere ocupa no texto. A chave, também chamada de *worm*, é uma string cujo comprimento determina os *blocos* em que o texto

simples é dividido. O *worm* é então repetidamente escrito sob a mensagem até cobrir todo o seu comprimento (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019). A Figura 4 elenca o esquema de criptografia.

Figura 4: Esquema de criptografia usando o método Vigenère

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Retirado de Encinas (2016)

Cada letra da mensagem deve ser substituída por outra de n-1 posições posteriores no alfabeto, onde n é o valor ordinal da letra correspondente na chave. A cifra pode ser considerada uma evolução do código de César, na verdade a cifra consistirá na soma módulo 26 (como para o código de César) de cada letra do texto simples com a letra subjacente da chave. Tem-se, então, "n" cifras de César, onde "n" é o comprimento da chave.

Deve-se notar que não há mais correspondência um-a-um entre os caracteres do texto em texto claro e do criptograma, não permitindo uma análise das frequências. Para decriptação, procede-se da mesma forma, ordenando repetidamente a chave sob o texto cifrado e executando a diferença módulo 26 (par a par) de caracteres (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; WAZLAWICK, 2016; PAPANI; SILVA, 2021).

Para facilitar a criptografia, Vigenère utiliza uma tabela na qual para encontrar o caractere criptografado é suficiente identificar o caractere em texto simples na primeira linha e, em seguida, o caractere do *worm* na primeira coluna. A interseção das duas

posições identificará automaticamente o caractere criptografado (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; SINGH, 2020; WAZLAWICK, 2016). Isto posto, examina-se a composição histórica da criptografia na idade moderna.

O monge franciscano Roger Bacon (1220 – 1292) escreveu o primeiro livro europeu onde se refere ao uso da criptografia, chamado *The Epistle on Secret Works of Art and the Nullity of Magic*, em que descreveu sete métodos diferentes para manter segredos em segredo. (WAZLAWICK, 2016). A grande maioria das pessoas se dedicava à criptografia, pois sabiam que as análises de frequência eram vulneráveis quando criptografadas. Foi assim que usaram duas cifras que lhes permitiram lutar contra o estudo das frequências, são elas: homófonos e nulos (WAZLAWICK, 2016).

As primeiras funcionam com os alfabetos normais (26 letras), mas são acrescentadas algumas letras novas, ou símbolos, tais como: ♦ ♣ ♥ ♠ que correspondem às letras mais frequentes. Por outro lado, na segunda criptografia, algumas letras sem sentido são incluídas na mensagem original e que não obstruem sua compreensão, é conveniente usar as letras nulas aquelas que têm pouca frequência para não alterar a mensagem. O Quadro 1 expõem as diferenças entre as duas.

Quadro 1: Tipos de Cifrado

Cifrado Homófono	Cifrado Nulo
Criptografando o seguinte texto: o rio está limpo se torna: Z ♠KZ FIDG ♣BMTS. Usando um alfabeto por substituição.	Criptografando a seguinte mensagem: a paz não foi assinada, quando a mensagem chega ao seu destino o decodificador não tem problemas para recuperar a mensagem original direta, tal como acima: A PAZ NÃO FOI ASSINADA.

Elaborado pela Autora (2022)

Como visto, nessa época, a criptografia era puramente baseada em cifras monoalfabéticas, o que se refere ao fato de que a substituição de chave, uma vez escolhida, não é modificada até que a criptografia da mensagem seja finalizada. Não devemos esquecer que também havia criptografias usando dois ou mais alfabetos, onde alternavam letra por letra para confundir o criptoanalista.

O anterior deu lugar a um grande salto qualitativo devido ao fato de passar de cifras monoalfabéticas a cifras polialfabéticas, onde León Battista Alberti (1402 – 1472) se destaca por criar a primeira máquina criptográfica composta por dois discos centrados

que giram independentemente, a fim de obter alfabeto de transposição em cada volta. Ele é considerado o avô da criptologia. A Figura 5 apresenta o Código Cifrado, finalizando estas análises iniciais.

Figura 5: Alfabetos

Alfabeto original	a	a	b	c	d	e	e	f	g	h	i	i	j	k	l	m	n	o	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	G	V	♦	X	C	♥	F	P	A	W	K	B	N	E	♣	M	L	Z	S	T	Q	♠	I	D	Y	O	R	J	U	H

Fonte: Elaborado pela Autora (2022)

1.4 Criptografia Moderna

Até a primeira metade do século XIX, a correspondência era exclusivamente em papel e entregue pelos correios. Entre a segunda metade do século XIX e o século XX, a invenção do telégrafo, do telefone e do rádio mudou radicalmente a forma de comunicação, possibilitando a transmissão de mensagens quase instantâneas mesmo de lugares muito distantes. Esses novos meios de comunicação, o rádio em particular, tornaram as interceptações de inimigos ainda mais fáceis e frequentes; o recurso à criptografia torna-se, portanto, inevitável, assim como a necessidade de cifras cada vez mais sofisticadas (ARAÚJO, 2018).

Em 1863, o coronel prussiano Friedrich Kasiski publicou o primeiro método de descriptografia da cifra de Vigenère com base na seguinte observação: porções repetidas de mensagens criptografadas com a mesma porção de chave resultam em segmentos de texto cifrados idênticos (ARAÚJO, 2018). Na Itália, a criptografia neste período é quase ignorada, será necessário esperar a entrada na guerra em 1915 para perceber o atraso acumulado no campo criptográfico e corrigi-lo. Nos EUA, os primeiros modelos iniciavam sua evolução. Já no Brasil, como se discute no próximo capítulo, iremos tratar sobre os primeiros passos de inovação tecnológica (ARAÚJO, 2018; WAZLAWICK, 2016).

Nesse mesmo tempo, no mundo, também foram desenvolvidas as primeiras máquinas de cifragem, que permitiram reduzir consideravelmente os tempos de cifragem e decifragem, transformando automaticamente as letras do texto claro nas do texto cifrado e vice-versa. Pode ser considerada a primeira e rudimentar máquina de criptografia de

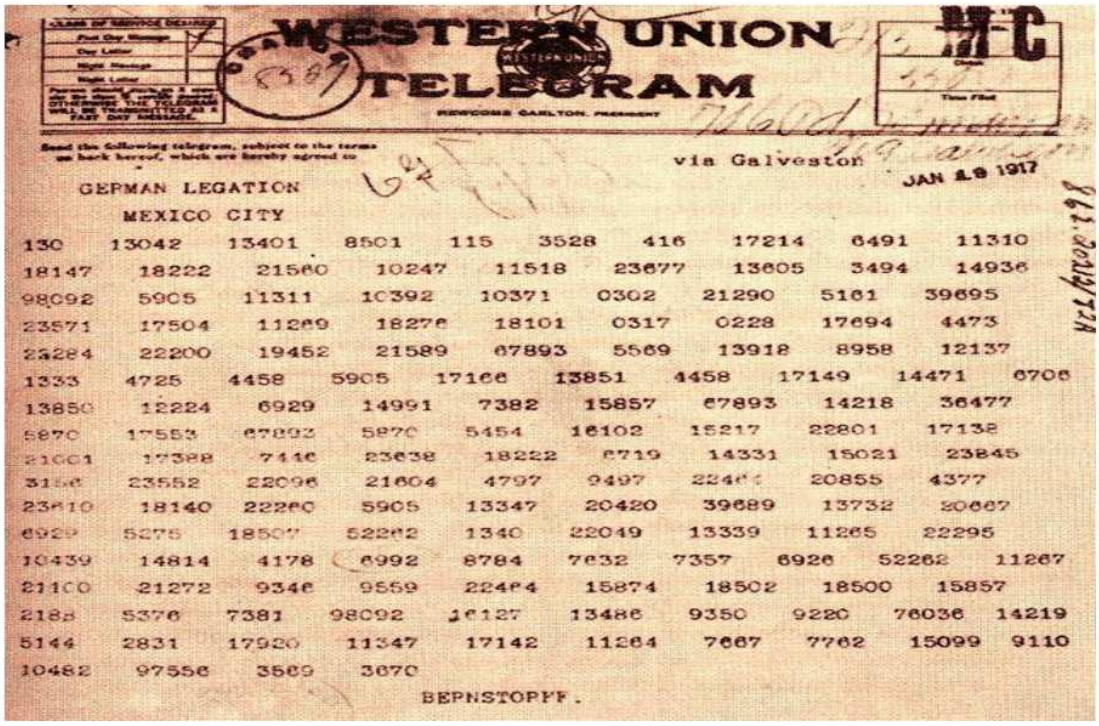
disco de Leon Battista Alberti, mas é na primeira metade do século XX que as máquinas de criptografia têm seu máximo desenvolvimento (WAZLAWICK, 2016; PRIETO, 2020). Um dos marcos fundamentais para quebrar o paradigma evolutivo da criptografia moderna, em todo o globo, foi a segunda guerra mundial, observada em frente.

Os franceses foram os primeiros a compreender as grandes mudanças provocadas pelas invenções do telégrafo e do rádio. No início da Primeira Guerra Mundial, já estavam organizados com um eficiente Gabinete de Cifras e em 1914 os criptoanalistas franceses conseguiram decifrar as mensagens de rádio alemãs. Mais um passo à frente dos franceses veio quando, em 1918, o melhor criptoanalista francês, o professor Georges Painvin, conseguiu decifrar a cifra de campo germânica, que era um método usado pelo exército alemão na Grande Guerra desde o início de 1918 (WAZLAWICK, 2016; BARCZAK, 2014).

Os únicos países organizados com escritórios de cifra reais no início da guerra eram a França e a Áustria, esta última já conseguindo decifrar as estações de rádio russas em 1914. Os russos, a princípio, nem se preocuparam em criptografar suas mensagens de rádio, permitindo assim que os alemães interceptassem qualquer informação e mesmo quando os russos começaram a usar mensagens criptografadas, os alemães conseguiram descriptografá-las. No Brasil, não foi muito diferente, com poucas evoluções – especialmente porque sua participação dentro da primeira guerra foi praticamente nula (PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010; WAZLAWICK, 2016).

Criptógrafos britânicos se reuniram na sala 40, o nome da sala do almirantado inglês onde está localizado o escritório criptográfico responsável pela violação dos códigos de cifra alemães. Milhares de mensagens de rádio da marinha alemã foram decifradas desta sala. O mais conhecido deles foi o *telegrama Zimmermann* com o qual os alemães ofereceram uma aliança aos mexicanos em uma chave anti-EUA. Lida no Congresso dos EUA, essa mensagem foi um dos fatores que levaram os EUA a entrar em guerra em 1917 (PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010; BARCZAK, 2014). A Figura 6 apresenta a imagem do telegrama, onde foi descriptografadas a mensagem de guerra.

Figura 6: telegrama Zimmermann (decifrado em meio à guerra)



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23038 18222 6719 14331 15021 23845
3156 23552 22098 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Fonte: Retirado de Código Espaguete (2021)

Nos EUA, o departamento de criptologia dos laboratórios Riverbanks em Chicago foi usado como escritório criptológico, no qual William Friedman também trabalhou, destinado a se tornar o maior criptologista e criptoanalista dos EUA. Completamente despreparados no campo da criptologia estavam os brasileiros e os países da América Latina, que inicialmente tiveram que confiar no escritório de cifras francês; só mais tarde foi criado um escritório autônomo, discutido em momento oportuno, que foi utilizado já na próxima guerra: Segunda Guerra Mundial (WAZLAWICK, 2016; BARCZAK, 2014). Em última análise, logo, foi a Grande Guerra que fez com que muitos estados descobrissem a importância da criptografia, cujo papel se tornará absolutamente fundamental na Segunda Guerra Mundial. Examinam-se os dois principais métodos da primeira grande guerra em frente.

O primeiro é o método Kasiski. O ataque Kasiski é baseado na observação de que sequências idênticas de caracteres são frequentemente encontradas a uma certa distância umas das outras em criptograma *viper*. De fato, a mesma letra do texto simples é geralmente criptografada com caracteres diferentes em suas várias ocorrências, mas se duas letras idênticas estiverem a uma distância igual à da chave, ou um múltiplo dela, elas serão criptografadas da mesma forma. Para identificar o comprimento da chave será,

portanto, suficiente calcular o máximo divisor comum entre as distâncias entre sequências repetidas. Uma vez encontrado o comprimento da chave, tendo um número significativo de criptogramas disponíveis, a análise de frequência pode ser aplicada a subconjuntos de caracteres que ocupam a mesma posição dentro de um bloco. Essa técnica também é chamada de método Babbage-Kasiski, pois, já em 1854, o excêntrico matemático e inventor Charles Babbage havia identificado um critério de decifração completamente semelhante ao desenvolvido posteriormente por Kasiski, mas nunca publicado (SANTOS, 2014). A Figura 7 apresenta a estrutura desse método.

Figura 7: Exemplo de Kasiski Cifrado

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	5	6	0	1	1	2	2	2	1	0	1	3	5	1	2	3	0	3	0	8	3	1	2	5	1	2
C2	9	1	0	2	0	1	0	9	4	3	1	1	0	2	5	5	0	0	1	0	5	3	0	0	4	4
C3	0	0	3	0	3	3	1	4	7	1	0	6	3	1	2	3	2	4	2	0	0	4	3	6	0	1
C4	0	0	6	2	1	3	9	2	0	6	2	0	0	2	2	1	1	1	0	5	4	6	3	0	2	1
C5	7	2	0	2	0	2	0	5	0	0	2	8	2	0	6	2	0	0	4	2	3	6	0	0	2	4
C6	2	0	0	0	5	2	0	4	3	1	0	4	4	1	0	5	2	3	4	1	0	2	5	7	4	0
C7	3	0	0	2	0	4	7	0	0	1	7	5	3	0	0	0	1	0	6	1	1	2	7	1	4	4
C8	8	1	2	1	0	1	0	5	3	3	4	3	1	4	4	5	2	1	1	3	2	2	0	0	1	2
C9	2	6	2	0	3	0	2	0	4	3	1	3	9	0	2	7	2	0	1	1	1	3	5	0	0	2
C10	1	1	1	2	3	5	0	0	3	1	6	2	1	0	0	2	0	6	3	2	3	8	0	2	4	3
C11	4	0	2	0	4	4	2	4	7	0	1	5	0	1	1	2	3	2	3	1	0	6	1	5	1	0
C12	1	0	3	1	0	2	9	0	0	11	3	1	0	2	4	2	7	1	0	0	4	3	1	1	3	0
C13	3	4	2	4	10	1	1	2	5	1	0	4	2	2	5	0	0	5	3	3	2	0	0	0	0	0
C14	2	2	1	1	2	3	4	4	0	0	5	5	4	0	0	4	0	1	0	4	1	1	2	9	1	3

Fonte: Elaborado pela Autora (2022)

O segundo é o Código Vernam, uma generalização do Código Vigenère, desenvolvido levando em consideração as fraquezas do código destacadas por Kasiski. Essas fraquezas do código Vigenère podem ser superadas alterando a chave com frequência e escolhendo chaves muito longas, como para cobrir qualquer mensagem que se espera que seja transmitida. Além disso, para tornar o método ainda mais seguro, as chaves podem ser geradas como sequências de letras, sem qualquer estrutura linguisticamente significativa. O código Vernam, também conhecido como *One Time Pad Code* (bloco descartável), prevê a edição tipográfica de blocos de papel idênticos, como um calendário destacável, com uma folha para cada dia, na qual longas sequências de caracteres aleatórios. O remetente e o destinatário têm um cadeado, que deve ser mantido em segredo, pois o cadeado mostra o conjunto de chaves a ser usado dia após dia (SANTOS, 2014; SINGH, 2011; LUNG, 2019).

A única maneira de decifrar a mensagem para o oponente é, portanto, dominar a chave; por esta razão o Vernam Code é o primeiro sistema criptográfico de chave simétrica totalmente seguro. Em 1949, Claude Shannon publicou a primeira prova matemática da inviolabilidade do Código Vernam, que, sendo o único sistema criptográfico cuja segurança é comprovada por uma prova, ganhou o título de *cifra perfeita.* No entanto, este esquema teoricamente perfeito é difícil de alcançar.

Na verdade, apresenta vários problemas práticos que não são fáceis de resolver. Em primeiro lugar, uma comunicação bastante massiva através do uso do código *One Time Pad* exigiria uma chave de tamanho desproporcional e isso agravaria ainda mais o problema de como trocar a chave entre remetente e destinatário.

Outra desvantagem desse sistema se dá pelo fato de que a chave utilizada deve ser gerada de forma totalmente aleatória, o que é praticamente impossível até hoje, na verdade os geradores de números aleatórios (por exemplo) são chamados de pseudo-casuais, pois geram números com propriedades que não são completamente aleatórias (SANTOS, 2014; SINGH, 2011; LUNG, 2019). A Figura 8 exemplifica.

Figura 8: Exemplo de Vernam

A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010

Fonte: Elaborado pela Autora (2022)

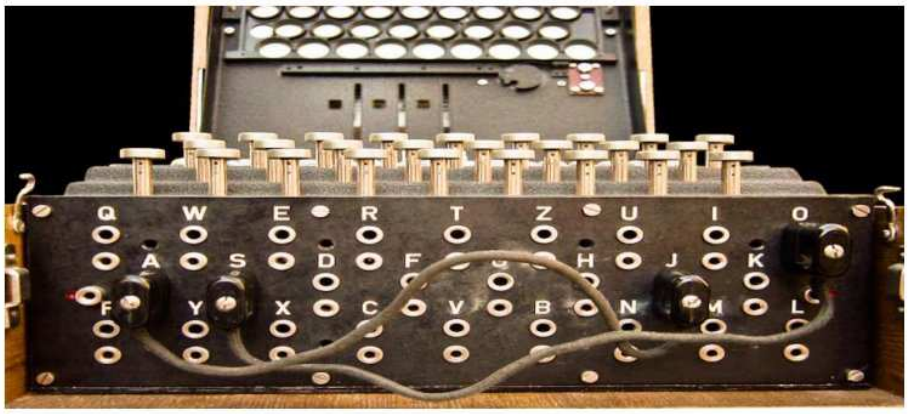
Vistos estes modelos, analisa-se o impacto da grande segunda guerra na evolução da criptografia. A busca por novos sistemas criptográficos deu um grande impulso à criptografia durante o período pré-Segunda Guerra Mundial. De fato, desde o início do século XX, nasceu a necessidade de poder usufruir de uma criptografia segura e, acima de tudo, rápida e fácil de usar: por isso nasceram as primeiras máquinas de

criptografia. Desde o final do século XIX, o desenvolvimento da criptografia tornou necessário automatizar progressivamente os métodos de criptografia e descriptografia, de modo que as máquinas de criptografia nasceram não tanto para tornar os sistemas criptográficos mais seguros, mas para acelerá-los. A primeira máquina de codificação foi inventada pelo comandante francês Étienne Bazeries já em 1891. A partir desta primeira máquina foram desenvolvidas muitas outras que permitiram métodos de criptografia cada vez mais rápidos e seguros; a mais famosa dessas máquinas é certamente a Enigma, patenteada pelo engenheiro alemão Arthur Scherbius em 1918 e adotada pelo exército e marinha alemães durante a Segunda Guerra (SANTOS, 2014).

O funcionamento destas máquinas baseia-se na utilização de um ou mais discos-cifras, também chamadas de rotores. Cada rotor tem uma permutação de 26 letras do alfabeto gravada nele e gira em torno de um eixo: isso permite que cada letra inserida seja criptografada com um alfabeto diferente. As máquinas de cifragem podem, portanto, ser consideradas uma versão mecânica da cifra de Vigenère. O rotor representa a principal característica das máquinas de criptografia, mas, ao mesmo tempo, também o ponto fraco, pois após 26 rotações o disco retorna à sua posição inicial. Uma máquina de cifragem de rotor único repete seu padrão de criptografia a cada 26 letras, tendo assim um período T = 26. É possível superar este problema adicionando mais rotores, uma máquina de 2 rotores, por exemplo, tem período 26 * 26 = 676 letras antes do texto ser criptografado com o mesmo padrão. Pode-se, portanto, dizer que a segurança aumenta exponencialmente com o aumento dos rotores e o período T de uma máquina com n rotores é igual a 26n (SINGH, 2011; SANTOS, 2014).

Em 1915, dois oficiais da marinha holandesa inventaram uma nova máquina para criptografar mensagens, destinada a se tornar uma das mais famosas de todos os tempos: a máquina de criptografia Enigma. Arthur Scherbius patenteou-a em 1918 e começou a vendê-la a bancos e empresas. O lugar da Enigma na história, porém, foi garantida em 1924, quando as forças armadas alemãs passaram a utilizar uma versão adaptada às necessidades militares para criptografar suas comunicações. E eles continuaram a confiar nessa máquina mesmo durante a Segunda Guerra Mundial, acreditando que ela era absolutamente segura (PAPANI; SILVA, 2021; COSTA; FIGUEIREDO, 2010). A Figura 9 apresenta uma imagem desta máquina, que é uma das mais referenciadas da idade atual.

Figura 9: Máquina de Criptografia Enigma



Fonte: Retirado de Papani; Silva (2021)

As máquinas Enigma na versão do exército tinham inicialmente três rotores que podiam ser extraídos e trocados. A primeira tarefa de um operador da Enigma era decidir em qual posição cada rotor individual deveria ser colocado. Havia cinco rotores para escolher e que poderiam caber nas três carcaças da Enigma (PAPANI; SILVA, 2021).

Cada caractere do texto simples era digitado em um teclado, a unidade de troca, composta principalmente por rotores, criptografava a letra transformando-a no elemento correspondente do criptograma e, por fim, uma lâmpada colocada no painel luminoso, acendendo, indicava a letra a ser incluída no criptograma (WAZLAWICK, 2016; PAPANI; SILVA, 2021; LUNG, 2019).

A peculiaridade do Enigma era que toda vez que uma letra era digitada no teclado, as partes móveis da máquina giravam, mudando sua posição para que um pressionamento subsequente da tecla correspondente à mesma letra fosse quase certamente criptografado de outra maneira. A máquina foi então enriquecida com um painel com múltiplos soquetes que permitia trocar pares de letras no início da codificação e um anel que regulava os tempos de rotação dos rotores. Tudo isso impossibilitou a criptoanálise pelos métodos tradicionais de análise de frequência e possibilitou que a Enigma permitisse um enorme número de chaves, ou seja, configurações iniciais da máquina (SINGH, 2011; LUNG, 2019).

A única maneira de descriptografar o criptograma era, portanto, ter uma máquina Enigma configurada exatamente como aquela com a qual a mensagem foi criptografada e digitar as letras no teclado, então as letras do texto simples acenderiam no painel. A configuração das máquinas alemãs era alterada a cada 24 horas seguindo um protocolo

específico a ser mantido em total sigilo, pois, se os aliados tivessem a posse, poderiam facilmente decifrar todas as mensagens (SINGH, 2011).

Até a primeira metade da década de 1920, os criptoanalistas americanos e franceses conseguiam descriptografar mensagens criptografadas pelos alemães com muita frequência. Isso só aconteceu até 1926, quando o uso massivo por parte dos alemães da Enigma, pôs em crise todo o aparato de contraespionagem britânico e francês (ENCINAS, 2016; PRIETO, 2020; WALLACE, 2019; LUNG, 2019).

O método criptográfico alemão parecia insuperável. Apenas poloneses, que sentiam os objetivos expansionistas da Alemanha contra eles, não desistiram. Muitos anos após o fim da guerra, soube-se que, de fato, já em 1932, o escritório de cifra polonês, liderado pelo matemático Rejewski, havia conseguido encontrar uma maneira de decifrar a máquina Enigma (ENCINAS, 2016).

Em agosto de 1939, os britânicos estabeleceram a escola de codificação e cifra em Betchley Park, onde recrutaram os melhores criptoanalistas, matemáticos e cientistas. Também explorando o conhecimento adquirido pelos aliados poloneses, durante a guerra, os britânicos continuaram a forçar sistematicamente as mensagens criptografadas com Enigma e, a partir de 1941, também as criptografadas com a mais sofisticada máquina de Lorenz (ENCINAS, 2016; ARAÚJO, 2018; SINGH, 2011).

A criptografia, portanto, desempenhou um papel de fundamental importância durante toda a duração da guerra e, por exemplo, foi fundamental para a invasão da Normandia no Dia D. De fato, Eisenhower e Montgomery foram capazes de ler todas as mensagens dos altos comandos alemães, que usavam a máquina de Lorenz; confirmaram assim que Hitler acreditara nas falsas notícias de um iminente desembarque aliado perto de Calais e concentrara suas melhores tropas naquela área. Eles foram então capazes de ordenar os desembarques na Normandia confiantes de que encontrariam pouca resistência (ARAÚJO, 2018; PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; LUNG, 2019).

Desde 1940, os americanos fabricavam o Magic, uma máquina capaz de descriptografar mensagens japonesas criptografadas com a máquina Purple. Isso permitiu, por exemplo, que os americanos vencessem a Batalha de Midway, conhecendo em detalhes os planos do exército japonês. É possível que os americanos também estivessem cientes do ataque de Pearl Arbor e decidissem não o impedir, talvez para convencer a opinião pública da necessidade de entrar na guerra (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; LUNG, 2019).

Uma teoria mais conservadora sustenta que os americanos sabiam que o Japão estava prestes a atacar, mas não sabiam onde (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; SINGH, 2020).

O que é certo é que no momento do ataque a Pearl Harbor não havia sequer um porta-aviões e, em última análise, apenas alguns navios antigos de importância não fundamental para a guerra foram afundados. No fim da guerra, o General Marshall admitiu que em muitos casos de importância *não vital,* os Aliados tinham que fingir não conhecer as mensagens criptografadas inimigas, mesmo ao custo de perdas humanas, como já retratado em diversos filmes relacionados com a temática, tal era o medo de que alemães e japoneses notassem que suas cifras estavam sendo sistematicamente descriptografadas (PRIETO, 2020; ENCINAS, 2016; WALLACE, 2019; SINGH, 2020; WAZLAWICK, 2016).

Cabe entrar ao Código Morse. Embora não seja considerado uma forma criptográfica, pois não está tentando ocultar uma mensagem, pode ser considerado um alfabeto alternativo que permite que as mensagens sejam transmitidas de forma mais simples. Para transmitir uma mensagem secreta usando esse tipo de código, o operador de telégrafo precisa criptografá-la antes de encaminhá-la. Não se pode esquecer que a cifra Vigènere se tornou a melhor forma de proteger mensagens secretas.

1.5 Criptografia Contemporânea

A criptografia contemporânea difere consideravelmente da criptografia de que se falou até agora devido ao advento dos computadores, que revolucionou profundamente tanto os sistemas criptográficos quanto a maneira de ver e usar a criptografia. Muitos sistemas criptográficos anteriormente analisados e considerados razoavelmente seguros até o século XIX, hoje, de fato, podem ser quebrados em demasiado pouco tempo graças à velocidade de processamento do computador.

Além disso, sistemas criptográficos complexos podem agora ser usados, mas, no passado, exigiriam tempos de criptografia muito longos manualmente (como DES e RSA), e grandes custos (PRIETO, 2020; ENCINAS, 2016).

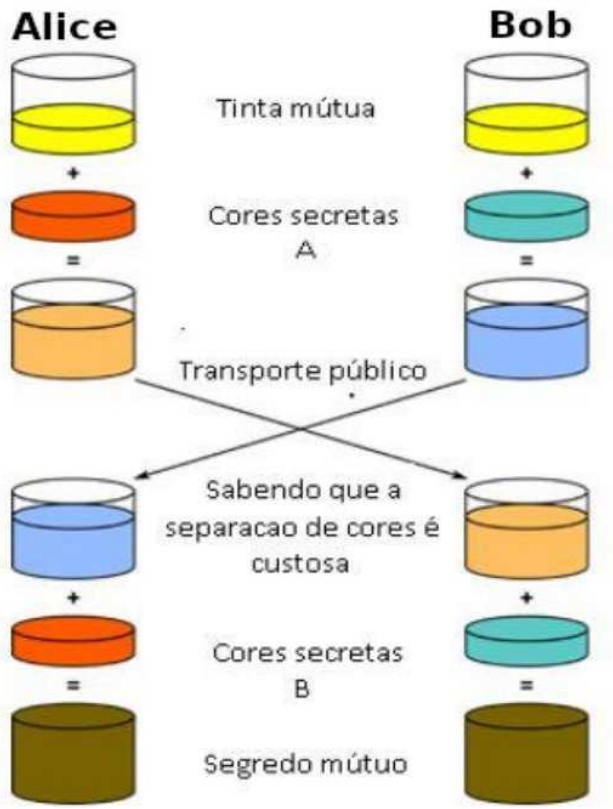
Na era da informática, a criptografia “saiu do campo de batalha” e é utilizada por todas as pessoas, mais ou menos conscientemente, no dia a dia: para sacar dinheiro em caixa eletrônico, ao fazer compras pela internet ou, simplesmente, ligar pelo celular e,

inclusive, até mesmo dentro do sistema de análise objeto desta pesquisa (sistema penitenciário).

A criptografia tornou-se, portanto, uma ferramenta de massa, projetada para proteger os segredos de estado tanto quanto os dados que se quer, ou pelo menos se gostaria, que permanecessem privados (WALLACE, 2019; SINGH, 2011). Em termos técnicos, dois são os modelos essenciais dos dias atuais: o código DES – um moderno sistema criptográfico de chave simétrica (a mesma chave para criptograr e descriptografar) –, e o método RSA que utiliza chave assimétrica.

O primeiro consiste prevê 128 caracteres dos quais apenas 96 são os chamados caracteres imprimíveis; cada caractere é codificado com um byte, ou seja, com 8 bits (dígitos binários 0,1). O texto simples é dividido em blocos, normalmente de 8 caracteres cada, escrever a codificação ASCII de cada bloco resultará em uma string de 64 dígitos. O segundo aplica um protocolo Diffie-Hellman (DH), em que cada usuário possui duas chaves distintas: uma pública e outra privada. A Figura 10 apresenta o protocolo DH.

Figura 10: Protocolo DH



Fonte: Adaptado de Papani; Silva (2021)

Já o último, RSA, é o sistema criptográfico de chave pública (assimétrica) mais conhecido e foi proposto pelos pesquisadores Rivest, Shamir e Adelman em 1978 (PRIETO, 2020; ENCINAS, 2016). Nessa pesquisa, não se entra diretamente no mérito de suas atividades e desenvolvimento de linguagem, haja vista que o objeto de trabalho se evidencia por meio do processo de criptografia observado nas outras áreas que foram avaliadas e não diretamente por uma perspectiva tecnológica. Isto é, na penitenciária, especialmente, são os modelos tradicionais e, até mesmo, rudimentares que são utilizados.

Capítulo II
Dos Computadores à Assinaturas Digitais

A era tecnológica, especialmente após os anos 2000, ganhou grande destaque em virtude das relações e das operações da sociedade, o que ocasionou a transformação das informações por meio do uso de criptografia. Neste capítulo, estes fatores são evidenciados em frente, à luz das utilizações contemporâneas.

2.1 Computadores e Representação da Informação

Os computadores, em definição clássica, são dispositivos eletrônicos que visam o armazenamento e processamento de dados, normalmente em forma binária, de acordo com as instruções dadas a ele em um programa variável. Assim, são estruturados em dois componentes: hardware (capacidade física) e software (programação), em que surgem os conceitos (COSTA; FIGUEIREDO, 2010).

Nesse sentido, o computador é um dispositivo eletrônico, assim, como um interruptor de luz, ele entende apenas dois estados. Acontece que isso é suficiente para fazer toda a ideia funcionar. De fato, qualquer sistema que possa representar pelo menos dois estados pode representar informação. Tome-se, por exemplo, o código Morse que é usado na telegrafia. Morse é um sistema de transmissão de som que pode levar um bipe curto (representado por um ponto) e um bipe longo (representado por um traço). Qualquer letra ou número pode ser representado por uma combinação desses dois símbolos (COSTA; FIGUEIREDO, 2010).

Da mesma forma com os computadores. Para representar um número, usamos o sistema aritmético binário, não o sistema de numeração decimal que se usa na vida cotidiana. No sistema binário, qualquer número pode ser representado usando apenas dois símbolos, 0 e 1, quase um Código Morse, mas não exatamente (devido às pausas entre as letras) um sistema binário. Um sistema intimamente relacionado ao Morse é usado por computadores para fazer compressão de dados (mais sobre isso mais tarde).

Nesta visão conceitual, a representação da informação é o uso de signos que substituem outra coisa. É por meio da representação que as pessoas organizam o mundo e a realidade pelo ato de nomear os seus elementos. Os signos são dispostos de forma a formar construções semânticas e expressar relações (GONÇALVES, 2003)

A representação tem sido associada à estética (arte) e à signos. Mitchell confirma que a representação é uma noção extremamente elástica, que se estende desde uma pedra que representa um homem até um romance que representa o dia na vida de vários dublinenses (nascidos em Dublin). O termo 'representação', assim, carrega uma gama de significados e interpretações. Na teoria literária, é comumente definida de três maneiras: para parecer ou assemelhar-se; para substituir algo ou alguém; e para apresentar uma segunda vez; para reapresentar. Pode ser utilizada em diversos dispositivos, modelos de comunicação, tal como os computadores (por seus códigos binários) e, em parte, pelos amplos modelos de criptografia, que utilizam diversas formas de representação (GONÇALVES, 2003). Dito isto, trazem-se algumas das principais categorizações de criptografia eletrônica nas seções em frente.

2.2 Chave Pública

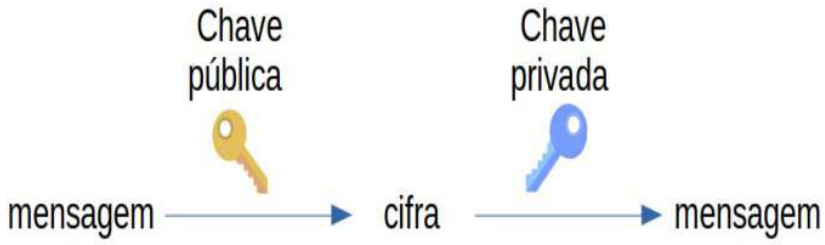
As implementações mais comumente usadas de criptografia de chave pública (também conhecida como criptografia de chave pública e criptografia assimétrica) são baseadas em algoritmos apresentados por Rivest-Shamir-Adelman (RSA) Data Security (COSTA; FIGUEIREDO, 2010).

A criptografia de chave pública envolve um par de chaves conhecidas como chave pública e chave privada (um par de chaves públicas), que estão associadas a uma entidade que precisa autenticar sua identidade eletronicamente ou assinar ou criptografar dados. Cada chave pública é publicada e a chave privada correspondente é mantida em segredo. Os dados criptografados com a chave pública podem ser descriptografados apenas com a chave privada correspondente (COSTA; FIGUEIREDO, 2010).

Os pares de chaves públicas RSA podem ser de qualquer tamanho. Os tamanhos típicos hoje são 1024 e 2048 bits. A criptografia de chave pública permite o seguinte: (a) criptografia e descriptografia, que permitem que duas partes comunicantes disfarcem os dados que enviam uma à outra. O remetente criptografa ou embaralha os dados antes de enviá-los. O receptor descriptografa ou decodifica os dados após recebê-los. Enquanto em trânsito, os dados criptografados não são compreendidos por um intruso; (b) o não repúdio, que impede: o remetente dos dados de alegar, posteriormente, que os dados nunca foram enviados e os dados de serem alterados (GONÇALVES, 2003). A Figura 11 mostra como se pode distribuir livremente a chave pública para que somente o

proprietário da chave privada) possa ler os dados que foram criptografados com a chave pública.

Figura 11: Exemplificação da Chave Pública



Fonte: Elaborado pela Autora (2022)

Em geral, para enviar dados criptografados para alguém, deve-se criptografar os dados com a chave pública dessa pessoa, e a pessoa que recebe os dados os descriptografa com a chave privada correspondente (COSTA; FIGUEIREDO, 2010). Se realizar uma comparação da criptografia de chave simétrica com a criptografia de chave pública, ver-se-á que a criptografia de chave pública requer mais cálculos. Portanto, a criptografia de chave pública nem sempre é apropriada às grandes quantidades de dados. No entanto, é possível usar a criptografia de chave pública para enviar uma chave simétrica, que pode ser usada para criptografar dados adicionais (BARCZAK, 2014; ARAÚJO, 2018).

O inverso do que é mostrado na Figura 11 anterior também funciona. Ou seja, os dados criptografados com sua chave privada podem ser descriptografados apenas com a chave pública. No entanto, essa não é uma maneira desejável de criptografar dados confidenciais porque significa que qualquer pessoa com a chave pública, que por definição é publicada, pode descriptografar dados confidenciais (BARCZAK, 2014; ARAÚJO, 2018). Apesar disso, a criptografia de chave privada é útil porque permite que se use sua chave privada para assinar dados com sua assinatura digital; qualquer pessoa com a chave pública pode ter certeza de que somente uma determinada enviou os dados). Este é um requisito importante para o comércio eletrônico e outras aplicações comerciais de criptografia e, inclusive, é um movimento que pode ser utilizado pelo crime organizado, ensejando mudanças nas composições de informação no sistema penitenciário (BARCZAK, 2014; ARAÚJO, 2018).

2.3 Certificados Digitais

Um certificado é um documento eletrônico usado para identificar um indivíduo, um servidor, uma empresa ou alguma outra entidade e associar essa identidade a uma chave pública. Como uma carteira de motorista, um passaporte, uma carteira de estudante, um cartão de biblioteca ou outras identificações pessoais comumente usadas, um certificado fornece uma prova geralmente reconhecida da identidade de uma pessoa. Os certificados usam criptografia de chave pública para resolver problema de representação (GONÇALVES, 2003).

Para obter uma carteira de motorista, normalmente se solicita ao Departamento de Veículos Motorizados, que verifica a identidade, a capacidade de dirigir, o endereço e outras informações pertinentes antes de emitir uma carteira de motorista. Para obter uma carteira de estudante, se inscreve em uma escola ou faculdade que, por sua vez, realiza verificações diferentes (como se você pagou sua mensalidade) antes de emitir a carteira de estudante. Para obter um cartão de biblioteca, só precisa fornecer o nome e uma conta de luz com endereço (COSTA; FIGUEIREDO, 2010). Os certificados funcionam da mesma forma que qualquer uma das formas de identificação mencionadas anteriormente. Autoridades de certificação (CAs) são entidades que validam identidades e emitem certificados. Clientes e servidores usam certificados emitidos pela CA para determinar os outros certificados que podem ser confiáveis (COSTA; FIGUEIREDO, 2010).

Assim como os métodos para validar outras formas de identificação podem variar dependendo de quem está emitindo o ID e da finalidade para a qual está sendo usado, os métodos usados para validar uma identidade podem variar dependendo das políticas de uma determinada CA. Em geral, antes de emitir um certificado, a CA deve usar seus procedimentos de verificação publicados para esse tipo de certificado para garantir que uma entidade que solicita um certificado seja, de fato, quem afirma ser (BARCZARK, 2014; ARAÚJO, 2018).

O certificado emitido pela CA vincula uma chave pública específica ao nome da entidade que o certificado identifica; por exemplo, o nome de um funcionário ou servidor. Os certificados ajudam a evitar o uso de chaves públicas falsas para representação. Somente a chave pública certificada pelo certificado funcionará com a chave privada correspondente de propriedade da entidade identificada pelo certificado (BARCZARK, 2014; ARAÚJO, 2018).

Além de uma chave pública, um certificado também inclui o nome da entidade que identifica, uma data de validade, o nome da CA que emitiu o certificado, um número de série e outras informações. Mais importante ainda, um certificado sempre inclui a assinatura digital da CA emissora. A assinatura digital da CA permite que o certificado funcione como uma carta de apresentação para usuários que conhecem e confiam na CA, mas não conhecem a entidade identificada pelo certificado. Certificados digitais, tão logo, aumentam a confiabilidade das informações que são repassadas por meio dos modelos eletrônicos, em que pese quaisquer que sejam as naturezas destas informações (BARCZARK, 2014; ARAÚJO, 2018). Tem-se como uma das ferramentas que mais popularizaram a criptografia nos últimos dias.

2.4 A Popularização da Criptografia nas Atividades Comerciais e Eletrônicas

No início da década de 1970, a criptologia era dominada pelos governos, tanto porque os computadores eram muito caros quanto pela necessidade de retenção de informações (COSTA; FIGUEIREDO, 2010; GONÇALVES, 2003).

Vários fatores empurraram a criptografia para que se tonar-se convencional. A mais importante delas foi a invenção da World Wide Web em 1989 e o uso generalizado de computadores. A comunicação industrial-comercial, como também a pessoal tinham que ser protegidas, por exemplo, os serviços financeiros foram alguns dos primeiros a exigir transações eletrônicas seguras. Outras empresas queriam proteger seus segredos comerciais armazenados digitalmente. Finalmente, os indivíduos queriam ter certeza de que sua comunicação online era segura. Hoje praticamente toda comunicação digital é, ou deveria ser, criptografada (GONÇALVES, 2003; COSTA; FIGUEIREDO, 2010; BARCZARK, 2014; ARAÚJO, 2018).

Na criptografia moderna, a segurança da criptografia não depende do método de criptografia (ou algoritmo), mas do sigilo das chaves usadas para criptografia e descriptografia. O brilhantismo do algoritmo RSA (em homenagem a seus inventores Ron Rivest, Adi Shamir e Leonard Adleman) está no uso de criptografia assimétrica para gerar um par de chaves pública e privada, ambos baseados em um algoritmo de grandes números primos (BARCZARK, 2014; ARAÚJO, 2018).

Para entender melhor como as chaves simétricas funcionam, deve-se lembrar da cítala usado pelos espartanos. A mensagem foi criptografada com o uso de um certo

comprimento e formato de cilindro, e tanto o remetente quanto o receptor tinham que ter o mesmo tipo de cilindro para criptografia e descriptografia. O problema começa quando a chave é comprometida, o que significa que o conteúdo da mensagem pode ser lido. Isso era menos arriscado com ferramentas físicas, mas muito mais fácil no mundo digital, permitindo que o remetente e o destinatário fossem explorados (BARCZARK, 2014; ARAÚJO, 2018).

A RSA introduziu o conceito de par de chaves pública-privada para criptografia. A chave pública é usada para criptografar os dados, que só podem ser descriptografados com a chave privada correspondente. Embora as duas chaves estejam matematicamente relacionadas, calcular a chave privada a partir do público é extremamente complexo e demorado, graças a um problema matemático chamado fatoração primária. O algoritmo RSA também estabeleceu as bases para métodos de autenticação modernos, pois o uso de um par de chaves pública-privada era perfeito para identificar se o remetente é quem ele diz ser e também garantia melhor segurança nas mensagens (COSTA; FIGUEIREDO, 2010; BARCZARK, 2014).

Nesse sentido, a criptografia moderna faz parte das vidas cotidianas e acontece a cada segundo sem que a maioria das pessoas esteja ciente disso. Mas por que a criptografia é usada com tanta frequência hoje em dia? Simplificando, não são mais apenas os humanos que se comunicam. Toda vez que um computador se conecta à Internet, você visita uma página da Web (HTTPS), usa um aplicativo de mensagens ou e-mail em seu telefone, computadores, dispositivos e software estão se comunicando entre si via Internet, Bluetooth, WiFi (COSTA; FIGUEIREDO, 2010). O problema é que os computadores também são muito bons em decifrar criptografia por causa do grande volume de operações matemáticas que podem ser concluídas em um segundo. Como resultado, proteger a Internet com criptografia moderna é complexo. Os métodos de criptografia devem ser sofisticados e rápidos o suficiente para proteger os canais nos quais ocorre a transferência de dados. Novos tipos de criptografia são baseados em problemas/algoritmos matemáticos complexos e implementam uma combinação de esquemas de criptografia de chave simétrica e assimétrica para proteger a comunicação (BARCZARK, 2014; ARAÚJO, 2018).

A geração de chave simétrica usa cifra de fluxo ou cifra de bloco. RC4 é a cifra de fluxo mais amplamente utilizada na qual um fluxo de números aleatórios é combinado com a mensagem original. A técnica é usada em Secure Socket Layer (SSL) e Wired

Equivalent Privacy (WEP) (GONÇALVES, 2003; BARCZARK, 2014; ARAÚJO, 2018; COSTA; FIGUEIREDO, 2010).

Os padrões de criptografia atuais adotados pelos governos e pela Agência de Segurança Nacional dos EUA, a principal agência tecnológica do mundo, geralmente são baseados na cifra de bloco AES, que criptografa um grupo de bits de comprimento fixo: ou seja, ele pega um texto simples de bloco de 128 bits e gera um texto cifrado do mesmo tamanho. Outras cifras de bloco populares são Blowfish, Twofish, DES. São, assim, os modelos de referência global (GONÇALVES, 2003). A autenticação segura (identificando um usuário e sua elegibilidade para acesso) e a certificação digital também são estabelecidas usando criptografia e chaves privadas, públicas e de sessão. Hypertext Transfer Protocol Secure (HTTPS) é uma extensão segura do protocolo HTTP (BARCZARK, 2014; ARAÚJO, 2018).

Nesse caso, o protocolo de comunicação usado na internet para acessar um site é criptografado usando o protocolo Transport Layer Security (TLS), que evita espionagem, adulteração, especialmente ataques man-in-the-middle. Enfim, todos os atos que podem ser estar direccionalmente observados por meio de atividades-crimes e de organizações criminosas, por consequência (GONÇALVES, 2003; BARCZARK, 2014; ARAÚJO, 2018). Finalizando esta análise, apresenta-se, na subseção em frente, a criptografia do sistema penitenciário.

2.5 A Relação da Criptografia com o Sistema Penitenciário

O foco dos sistemas penitenciários está diretamente nas investigações criminais e não em operações de inteligência aplicada. Com isto, cada vez mais, o sistema se mostra defasado com as alterações e atualizações do crime organizado. Casos reais envolvendo criptografia fornecem informações sobre o escopo do problema e os métodos usados pelas autoridades para lidar com ela. As descobertas desses casos sugerem que o número total de casos criminais envolvendo criptografia em todo o mundo é de 500 e que poucos são os recursos do sistema penitenciário para convalidar as dificuldades destas atribuições (GONÇALVES, 2003).

Em geral, na relação com a segurança pública e do sistema penitenciário, a ameaça representada pela criptografia para a aplicação da lei, segurança pública e segurança nacional se manifesta de várias maneiras: falha na obtenção de provas necessárias para investigações criminais, falha para evitar ataques catastróficos ou prejudiciais, e a falha

na obtenção de informações estrangeiras vitais para a segurança nacional (BARCZARK, 2014; ARAÚJO, 2018; GONÇALVES, 2003). A criptografia também pode atrasar investigações criminais, aumentar seus custos e exigir o uso de métodos investigativos que podem ser perigosos ou invadir a privacidade, o que torna, de fato, importante estudar suas atribuições (BARCZARK, 2014; ARAÚJO, 2018; GONÇALVES, 2003).

As tendências no mercado de criptografia que preocupam a aplicação da lei incluem a crescente integração de criptografia extremamente forte em aplicativos e redes comerciais de desktop e o crescente mercado de sistemas de recuperação de chaves que protegem os proprietários de dados criptografados contra chaves perdidas (BARCZARK, 2014; ARAÚJO, 2018; GONÇALVES, 2003). Outras ferramentas que podem ser aprimoradas pela criptografia, incluindo telefones celulares clonados e esteganografia, podem ser usadas para evitar a detecção policial, conduzir vigilância e invadir computadores e redes (GONÇALVES, 2003).

As opções de política de criptografia devem ser discutidas no que diz respeito aos controles e regulamentos de exportação, e o programa de criptografia brasileiro em que pese seu sistema penitenciário deve promover tecnologias de recuperação de chave por meio de controles de exportação liberalizados, padrões de recuperação de chave e um regime de licenciamento voluntário para agentes de recuperação de chave é revisado, o que ainda não é visto na realidade brasileira, implicando no aumento desproporcional do crime organizado e das ferramentas destes em face do sistema penitenciário brasileiro. (BARCZARK, 2014; ARAÚJO, 2018; GONÇALVES, 2003). Dito isto, muitas são as tecnologias em criptografias, mas à luz da disposição da justiça, parecem significativamente escassas.

Capítulo III
Sistema Penitenciário Brasileiro

O terceiro capítulo faz uma explanação sobre o ambiente que se dá o objeto dessa pesquisa, mencionando as principais organizações criminosas atuantes no sistema prisional brasileiro e como o sistema de inteligência atua no combate a essas organizações.

3.1 Execução Penal No Brasil

A execução penal no Brasil é regulamentada pela Lei nº 7.210, de 11 de julho de 1984 (BRASIL, 1984). Antes disso, havia um regime penal, processual e penitenciário conformado ao pensamento e experiência europeus, que em muitos aspectos se desviava da realidade brasileira, à criação de um corpo diretivo para a política carcerária nacional, mais ligado às características específicas do país.

A primeira tentativa de consolidação das regras de execução penal no Brasil ocorreu com o anteprojeto do Código Penitenciário da República, em 1933, cuja discussão foi impedida com o advento do Estado Novo. No período republicano, apesar das discussões sobre a constitucionalidade da iniciativa da União de legislar sobre a matéria, foi aprovada a Lei nº 3.274, de 2 de outubro de 1957, que estabeleceu regras gerais aplicáveis ao sistema prisional. A lei era bastante avançada para a época, pois continha normas relacionadas à dignidade e ao exercício dos direitos dos presos. No entanto, esta lei foi rapidamente considerada ineficaz porque não impunha, de fato, sanções significativas pelo descumprimento das normas estabelecidas (RIBEIRO, 2019; GONÇALVES, 2003).

Em 1963, foi elaborado o anteprojeto de um Código de Execuções Penais, mas não prosperou devido ao Golpe Militar de 1964, que implantou a ditadura no Brasil, e também porque o debate sobre a constitucionalidade da iniciativa da União de legislar sobre as normas jurídicas fundamentais do sistema penitenciário. Na década de 1970, foi elaborado um novo anteprojeto do Código de Execuções Penais, que também não viu a luz do dia. Finalmente, em 1981, após o 1º Congresso Brasileiro de Política Criminal e Penitenciária, uma comissão de juristas se encarregou de elaborar outro projeto de Lei de Execução Penal, que se tornou a ainda atual Lei nº 7.210/1984 (RIBEIRO, 2019).

A Lei nº 7.210/1984, passou a fazer parte da Lei de Execução Penal, de forma a abranger tanto a regulamentação do Direito Penitenciário, uma vez que regulamenta a gestão administrativa dos estabelecimentos penitenciários, a prática de atos inerentes à cumprimento da pena e dos direitos e deveres dos reclusos; bem como o Direito Processual Penal, disciplinando a atuação jurisdicional. O então Ministro da Justiça Ibrahim Abi-Ackel, responsável pela redação da Declaração de Motivos da LEP, defendeu a autonomia científica da Lei de Execução Penal por não ter natureza predominantemente administrativa e, apesar de relacionada, não ser o mesmo que Direito Penal e Processo Penal (RIBEIRO, 2019).

Segundo o Ministro, no entanto, como não se trata de um regulamento penitenciário ou de um estatuto do preso, evoca todo o conjunto de princípios e normas que delimitam e jurisdicionam as medidas de reação penal. A execução de penas e medidas de segurança deixa de ser um Livro do Código Processual, entrando nos costumes jurídicos do país com a autonomia inerente à dignidade de um novo ramo jurídico: a Lei de Execução Penal.

Portanto, a Lei de Execução Penal trata de todas as questões relacionadas à execução da pena, mantendo estreita relação com o Direito Constitucional, pois estabelece direitos e garantias individuais e limita a pretensão punitiva do Estado. Relaciona-se também ao Direito Penal, pois disciplina diversos institutos vinculados à execução da pena; e com o Direito Processual Penal, considerando que o processo penal utiliza princípios, normas, teorias e jurisprudências para buscar o equilíbrio entre o direito de punir do Estado e o direito de defesa do réu. Além disso, esse ramo é constituído por normas jurídicas nos sentidos material e formal, ou apenas material, incluindo, além das leis, a edição de atos normativos no âmbito do DEPEN, dos departamentos penitenciárias locais e até mesmo diretores de prisões, delimitando condutas bem como reduções e benefícios aos próprios indivíduos em execução.

O artigo 1º da LEP trata da sua finalidade e alcance ao prever que "A execução penal tem por objeto cumprir o disposto em sentença ou decisão penal e proporcionar condições para a integração social e harmoniosa do condenado" (BRASIL, 1984).

Entende-se por execução penal o conjunto de regras e princípios que visam tornar efetiva a decisão judicial, podendo impor pena privativa de liberdade, restritiva de direitos ou multa ao acusado e, ainda, a aplicação de medida de segurança, consistindo em tratamento ambulatorial ou internação em hospital de custódia e tratamento psiquiátrico (RIBEIRO, 2019).

Na parte final do artigo analisado, nota-se que a LEP visa também a recuperação dos condenados, para que não cometam mais crimes quando retornarem ao convívio social. Por isso, a lei consagra o direito do condenado a estudar e trabalhar (SENNA, 2020).

Ratificando esse entendimento, a seção Motivos da LEP estabelece que O artigo 1º contém duas ordens de finalidade: a correta execução das ordens existentes em sentenças ou outras decisões, destinadas a reprimir e prevenir crimes, e a provisão de meios pelos quais presos e sujeitos a medidas de segurança ter uma participação construtiva na comunhão social. (...) as penas e medidas de segurança devem realizar a proteção do patrimônio legal e a reincorporação do autor à comunidade" (BRASIL, 1984).

A doutrina não é pacífica quanto à natureza jurídica da execução penal. Há quem entenda ter caráter puramente administrativo e quem defenda seu caráter eminentemente jurisdicional. A orientação de que se trata de uma atividade complexa, desenvolvida tanto na esfera administrativa quanto na jurisdicional, parece mais coerente, pois algumas medidas podem ser adotadas pelo diretor da penitenciária, enquanto outras só podem ser tomadas pelo Juiz. São estas medidas – em relação aos gestores e diretores (bem como funcionários) (RIBEIRO, 2019), que também se buscam ser avaliadas ao longo desta pesquisa.

Em todo caso, a finalidade da execução penal é ao mesmo tempo punir e humanizar, em contratempo busca ressarcir o mal causado pela infração penal com a sanção (função retributiva), também tem o objetivo de recuperar e reinserir o infrator na sociedade (função preventiva), avaliar a sua conduta e compreender quais as necessidades para realinhar o indivíduo com a sociedade. Todavia, segundo Senna (2020), mais parece que o sistema penitenciário corrompe do que restitui o indivíduo para o convívio em sociedade e coletivismo. Isto posto, em frente, apresenta-se a estrutura geral sistema penitenciário brasileiro, tendo como foco as penitenciárias estaduais, à luz da execução penal.

3.1.1 Carceragem no Brasil: Estrutura Contemporânea

Com cerca de 680.000 detentos espalhados por cerca de 500 prisões, milhares de carceragens policiais e inúmeras outras instalações, o Brasil administra um dos dez

maiores sistemas penais do mundo com proporção relativamente moderada, no entanto. Com cerca de 320 presos por 100.000 habitantes, o Brasil encarcera menos pessoas per capita do que muitos outros países da região, e muito menos do que os Estados Unidos (SENNA, 2020).

No campo das instalações penais, a população carcerária do Brasil está distribuída entre várias categorias de estabelecimentos, incluindo penitenciárias e presídios, cadeias públicas, casas de detenção e delegacias de polícia. A lei penitenciária nacional exige que várias categorias de estabelecimentos sejam identificáveis por características específicas e mantenham tipos específicos de presos. Na prática, porém, essas categorias são demasiadas mais maleáveis e intercambiáveis do que a lei sugere (TEIXEIRA, 2018).

Em teoria, o percurso de um preso pelo sistema penal deve seguir um curso previsível: após a prisão, o suspeito do crime deve ser levado a uma carceragem da polícia para registro e detenção inicial. Dentro de alguns dias, se ele não for solto, ele deve ser transferido para uma prisão ou casa de detenção para aguardar julgamento e sentença. Se condenado, ele deve ser transferido para uma instalação específica para presos condenados. Ele pode passar suas primeiras semanas ou meses após a condenação em um centro de observação, onde um corpo de pessoal treinado estuda seu comportamento e atitudes - entrevistando-o, fazendo-lhe exames de personalidade e criminológicos e obtendo uma série de informações sobre ele - para selecionar a prisão ou outro estabelecimento penal mais bem equipado para reformar suas tendências criminosas (SENA, 2020).

De acordo com a lei penitenciária nacional, as instalações para presos condenados se enquadram em três categorias básicas: instalações fechadas, ou seja, prisões; instalações semiabertas, que incluem colônias agrícolas e industriais; e instalações abertas, ou seja, casas de passagem. Um preso condenado seria transferido para uma dessas instalações de acordo com sua duração da pena, tipo de crime, periculosidade percebida e outras características. No entanto, se começar a cumprir a pena numa prisão, deverá normalmente ser transferido para um estabelecimento de tipo menos restritivo antes de cumprir a sua pena, permitindo-lhe habituar-se a uma maior liberdade – e, idealmente, a adquirir competências úteis – antes de cumprir a pena e atingir sua libertação na sociedade (BECCARIA, 2020).

Como esta seção descreve, a realidade no Brasil está muito distante das prescrições da lei. Para começar, o sistema penal do país carece da infraestrutura física necessária para garantir o cumprimento da lei (o que também causa impacto na

supremacia dos modelos de criptografia que existe). Em muitos estados, por exemplo, casas de passagem simplesmente não existem; em outros lugares, eles não têm capacidade suficiente para lidar com o número de presos. As colônias agrícolas são igualmente raras. De fato, como será descrito mais detalhadamente abaixo, não há nem de perto espaços prisionais suficientes para lidar com o número de detentos que chegam, forçando muitos presos condenados a permanecer por anos em carceragens de polícia, o que implica em menor possibilidade de mitigar risco entre presos, como a troca de informações para crime organizado (SENNA, 2020).

As instalações penais do Brasil estão espalhadas por todo o país, mas estão mais concentradas dentro e ao redor de áreas urbanas e em regiões densamente povoadas. São Paulo, o estado mais populoso do Brasil (que engloba a cidade de São Paulo, sua maior cidade), tem de longe a maior população carcerária. De fato, apenas São Paulo detém cerca de 40% dos presos do país, uma população carcerária maior do que a encontrada na maioria dos países latino-americanos. Outros estados com populações carcerárias significativas incluem, em ordem decrescente de magnitude, Rio de Janeiro, Minas Gerais, Rio Grande do Sul, Paraná e Pernambuco (BECCARIA, 2020).

Oito dos vinte e seis estados do Brasil, em contraste, cada um confina menos de mil prisioneiros. Entre eles estão vários estados com as menores taxas de encarceramento; em outras palavras, suas pequenas populações carcerárias não apenas refletem seu pequeno número de habitantes, mas também que aprisionam uma proporção relativamente pequena de pessoas. Alagoas, por exemplo, tinha uma taxa de encarceramento de 17,8 presos por 100.000 habitantes em 1995 – a menor taxa do Brasil – de modo que confinou apenas 478 pessoas, embora esteja no meio entre os estados brasileiros em termos de população total (SENNA, 2020; MINHOTO, 2021; RIBEIRO, 2019).

O Brasil, de fato, não tem um sistema penal, mas muitos. Como os Estados Unidos e outros países federais, embora diferentemente da maioria dos países latino-americanos, as prisões, cadeias e carceragens policiais do Brasil são administradas por seus governos estaduais. Ou seja, cada um dos vinte e seis governos estaduais, bem como o governo do Distrito Federal, administra um conjunto separado de estabelecimentos penais com uma estrutura organizacional distinta, políticas independentes e, em alguns casos, uma lei prisional complementar, como seus níveis de superlotação prisional, custos mensais por detento e salários dos guardas (SENNA, 2020; MINHOTO, 2021; RIBEIRO, 2019).

A estrutura dos sistemas penais estaduais não segue um modelo rígido. Mais comumente, o poder executivo estadual, que é chefiado pelo governador do estado, administra o sistema prisional por meio de sua secretaria de justiça, enquanto sua secretaria de segurança pública, órgão responsável pela polícia, geralmente controla as carceragens policiais. (Instalações nominalmente chamadas de cadeias públicas ou cadeiões) podem se enquadrar em qualquer uma das secretarias. No entanto, há muitas exceções a essa regra geral. No estado de São Paulo, mais notavelmente, o sistema prisional tem sua própria secretaria, conforme recomendado na lei penitenciária nacional de segurança (TEIXEIRA, 2018).

De acordo com a lei penitenciária nacional, as responsabilidades judiciais em relação aos presos não terminam na sentença. Ao contrário, os juízes têm a obrigação central de conduzir os presos pelas várias etapas do sistema penal (SENNA, 2020; MINHOTO, 2021; RIBEIRO, 2019; MACHADO; GUIMARÃES, 2014). Todavia, o problema se concentra exatamente nessa área de execução, onde há lacunas de investigação e de atividades para reduzir a comunicação entre os presos e o mundo exterior. Juntando estas lacunas como o atual sistema que não comporta os prisioneiros, o crime organizado ganha cada vez mais espaço dentro da carceragem brasileira, onde organizações centralizadas criminosas conseguem realizar toda a sua administração mesmo de dentro das celas. Frente a isto, a próxima seção avalia as principais organizações presentes na carceragem brasileira.

3.2 Organizações Criminosas

As duas principais organizações criminosas, que apresentam subconjuntos de organizações em suas estruturas, dentro da perspectiva Brasil, são o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV). Nesta seção, avaliam-se seu contexto histórico e sua presença nos dias atuais na carceragem brasileira. Em relação ao primeiro, há muitas versões diferentes do chamado fundador do Primeiro Comando da Capital, mas parece que a mais crível foi apresentada pelo jornalista investigativo Josmar Jozino em seu texto Cobras e Lagartos, de 2004. Segundo essa versão, a quadrilha foi formada em 31 de agosto de 1993 no presídio de Taubaté, na cidade de São Paulo, inspirada por um grupo de detentos de um time de futebol chamado Primeiro Comando da Capital, que planejava partida com outro rival chamado Comando Caipira (INSIGHT CRIME, 2020).

A partida nunca aconteceu porque membros da equipe do Primeiro Comando da Capital assassinaram dois de seus rivais, cortaram suas cabeças e os jogaram no campo de jogo para proclamar que a partir de agora eles seriam os donos do presídio. Há um claro paralelo aqui com os primeiros dias do cartel de drogas mexicano La Familia Michoacana, cujos sanguinários jogaram as cabeças decepadas de seus rivais na pista de dança de uma discoteca em Uruapan em 2006 (COUTINHO, 2019). Inicialmente, o objetivo do Primeiro Comando da Capital era proteger os integrantes de represálias de guardas e policiais ou ataques de outras quadrilhas prisionais, dar apoio às famílias dos presos e simpatizantes da quadrilha e estabelecer uma rede de comunicação entre membros de gangues encarcerados em diferentes prisões. A ideia promovida era evitar que outro massacre do Carandiru acontecesse e lutar para melhorar as condições de vida dos presos e a solidariedade contra a violência policial branca contra os afro-brasileiros (BENJAMIN, 2016). Devido à ação tardia e ineficaz das autoridades paulistas e à política de marginalização pretendida da ameaça por parte das autoridades federais, o Primeiro Comando da Capital ganhou a oportunidade de se expandir primeiro em outros presídios do estado de São Paulo, e depois em outras partes do Brasil, exterminando rivais e ganhando apoio para sua posição dominante na comunidade carcerária (COUTINHO, 2019).

Essa estratégia foi bem-sucedida e em poucos anos o Primeiro Comando da Capital começou a assumir o controle das prisões em todo o estado de São Paulo. Além disso, a quadrilha do PCC usou sua posição para legitimar suas ações, entre outras coisas, criando um novo código de lei para regular o comportamento dos presos, mediando negociações entre presos e autoridades prisionais, impedindo a escalada entre presos e funcionários da prisão e monopolizando o uso de violência por detentos em prisões controladas. O Primeiro Comando da Capital disseminou o uso de celulares entre seus integrantes em diversos presídios, facilitando muito a coordenação das operações criminosas da quadrilha. Deve-se notar que houve uma disputa de poder entre duas facções do próprio Primeiro Comando da Capital: os membros fundadores e a nova geração (INSIGHT CRIME, 2020).

O líder desta última facção é Marcos Willians Herbas Camacho, o Marcola, e a rivalidade levou a uma rebelião no presídio de Taubaté em dezembro de 1999. Durante a rebelião, os aliados de Marcola conseguiram assassinar a maioria dos os membros fundadores do PCC, fortalecendo assim sua própria influência dentro da estrutura de gangues. Por volta de 2001, as autoridades estaduais decidiram transferir cinco lideranças

do Primeiro Comando da Capital para o presídio de Taubaté. Ao mesmo tempo, as autoridades transferiram comandantes e membros mais importantes do PCC para presídios da periferia ou para outros estados, a fim de enfraquecer o PCC dessa forma. Tudo isso contribuiu para a eclosão da primeira mega-rebelião, que ocorreu em fevereiro de 2001 (LARKINS, 2021; BENJAMIN, 2016).

Os membros das gangues não apenas tomaram o controle das prisões, exibindo faixas ou pichando indicando sua filiação criminosa, mas também fizeram milhares de reféns entre as pessoas visitando seus entes queridos nas prisões. Este evento foi uma excelente demonstração do poder do Primeiro Comando da Capital e suas capacidades não apenas contra rivais, forças de segurança e autoridades, mas também para um público, que até então desconhecia a ameaça que a quadrilha do PCC poderia gerar. A quadrilha não apenas consolidou seu domínio e controle nos presídios do estado de São Paulo, mas conseguiu fortalecer a lealdade e a identificação entre seus próprios membros (COUTINHO, 2019).

O desafio lançado pelo Primeiro Comando da Capital não ficou sem resposta pelas autoridades estaduais. Já em maio de 2001, as leis prisionais foram endurecidas com a introdução do Regime Disciplinar Diferenciado (RDD), que permitiu, entre outras coisas, restrições às visitas conjugais, acesso à mídia e licenças para presos problemáticos e confinamento temporário. Também foi projetado para isolar os líderes do PCC para impedi-los de dirigir as operações criminosas da quadrilha. Além disso, a nova lei fortaleceu a vigilância dos presos por meio da atualização dos sistemas de monitoramento. Políticas carcerárias mais restritivas levaram a um aumento acentuado do número de presos no estado de São Paulo. Desse contexto histórico, o PCC ganhou roupagem no Brasil todo, disseminando-se de norte a sul com uma posição de front-*runner* nos presídios da região sudeste no Brasil, isto é, São Paulo e Rio de Janeiro. Em frente, trabalham-se as questões históricas desta facção na geografia brasileira e nos cenário político-econômico atual (INSIGHT CRIME, 2020).

A modernização do Primeiro Comando da Capital permitiu que a quadrilha continuasse a se expandir. Os membros do PCC provocavam intencionalmente pequenos tumultos em centros correcionais para que as autoridades estaduais os transferissem para presídios distantes e depois para presídios em outros estados, onde o Primeiro Comando da Capital ainda não tinha influência. Devido a tais decisões das autoridades, a expansão da quadrilha foi rápida, o que permitiria desenvolver operações cada vez mais extensas no futuro. Por exemplo, já em 7 de março de 2002, o PCC realizou o primeiro atentado

terrorista em São Paulo, explodindo um carro com 40 quilos de explosivos próximo ao Fórum Barra Funda, onde trabalhavam cinco mil pessoas. Felizmente, ninguém foi morto. Além disso, membros do Primeiro Comando da Capital tentaram influenciar o resultado da eleição para governador do estado de São Paulo em 2002, entre outras coisas, fazendo com que suas famílias votassem no candidato apoiado por gangues no primeiro turno (BENJAMIN, 2016).

No segundo turno, líderes do sindicato da morte do PCC planejaram um bombardeio malsucedido à bolsa de valores para minar o apoio ao candidato de direita e ao mesmo tempo influenciar a eleição presidencial. Além disso, em março de 2003, membros de gangues do PCC mataram dois juízes encarregados da segurança de presídios nos estados de São Paulo e Espírito Santo. Além disso, naquele mesmo ano, o Primeiro Comando da Capital lançou um ataque a aproximadamente 50 delegacias, durante o qual, bandidos assassinaram três policiais. E em agosto de 2005, acredita-se que membros do Sindicato da Morte do PCC tenham roubado mais de US$ 70 milhões do Banco Central na cidade de Fortaleza (COUTINHO, 2019).

O ano de 2006 viu a verdadeira escala da ameaça representada pelo Primeiro Comando da Capital, bem como o fracasso total tanto do sistema Regime Disciplinar Diferenciado quanto da política de marginalização da crescente quadrilha do PCC. De março a maio de 2006, ocorreram 82 revoltas prisionais não só no estado de São Paulo, mas também em estados vizinhos. Em maio de 2006, as autoridades federais decidiram transferir cerca de 750 integrantes do PCC encarcerados na cidade de São Paulo para presídios de segurança máxima do interior. Essa medida, prevista para 14 de maio de 2006, tinha como objetivo enfraquecer a influência do PCC e evitar novas rebeliões. Graças a um funcionário corrupto com acesso a documentos do Congresso, os líderes das quadrilhas do PCC souberam dos planos de enfraquecimento do PCC já em 10 de maio (COUTINHO, 2019).

Marcola tomou a decisão de começar a confrontar as autoridades estaduais alguns dias antes para surpreender as autoridades. Assim, em 12 de maio de 2006, teve início a operação cuidadosamente planejada do Primeiro Comando da Capital, que se transformou em confrontos entre membros de gangues e forças de segurança, a segunda mega-rebelião. As ações dos membros da quadrilha não apenas incutiram terror e levaram a uma escalada de violência, mas também paralisaram a cidade de São Paulo. Por cerca de uma semana, escolas, universidades, shopping centers, empresas e lojas foram fechadas com vendas no varejo caindo 90% durante esse período (INSIGHT CRIME, 2020).

Além disso, membros de gangues do PCC lançaram 293 ataques a delegacias de polícia e prédios públicos e queimaram mais de 100 ônibus em nove dias. Além disso, membros do Primeiro Comando da Capital realizaram atentados a bomba ou ataques com granadas em delegacias de polícia, bancos, escritórios de empresas importantes e uma estação de metrô. Gângsteres pertencentes ao PCC realizaram execuções nas ruas de policiais e guardas prisionais em estabelecimentos correcionais, além de assassinar civis (LARKINS, 2021).

As autoridades estaduais, surpresas, reagiram reforçando a força policial na cidade e convocando esquadrões da morte, o que alimentou a espiral de violência. O agravamento da situação na cidade de São Paulo obrigou as autoridades a entrar em negociações secretas com os líderes do Primeiro Comando da Capital. Em uma reunião informal com autoridades estaduais em 15 de maio de 2006, Marcola exigiu, entre outras coisas, mais direitos para os presos e garantias de que uma unidade especial de polícia para reprimir rebelião nas prisões chamada Tropa de Choque não teria acesso às prisões. As autoridades do Estado de São Paulo concordaram com as condições do líder do Primeiro Comando da Capital e assim, em 17 de maio de 2006, a quadrilha encerrou sua operação. Deve-se notar que de 492 a 505 civis foram mortos pela quadrilha. Além disso, a escala de terror e violência desencadeada pelo PCC levou a uma significativa erosão do respeito público às autoridades estaduais e ao próprio governador de São Paulo Geraldo Alckmin – um defensor de políticas restritivas adepto de políticas carcerárias restritivas – e consolidou a dominação do PCC entre outras quadrilhas do estado de São Paulo. A partir de agora, autoridades estaduais terão que levar em conta os interesses das lideranças do Primeiro Comando da Capital na hora de criar política (INSIGHT CRIME, 2020).

À medida que a quadrilha do PCC continuou a crescer e aumentar sua influência não apenas no estado de São Paulo, mas também nos estados vizinhos, ganhou a oportunidade de um envolvimento mais sério no narconegócio e na expansão internacional. Em 2010, o PCC havia expandido sua influência no oeste (Paraná, Mato Grosso do Sul e Mato Grosso) e no norte (Rondônia, Acre e Roraima) do Brasil, sem romper a esfera de influência de seu aliado, o Comando Vermelho. A crescente atividade criminosa do PCC nos estados brasileiros de fronteira com importantes rotas de contrabando não ficou sem resposta das autoridades, que se concentraram em prender e encarcerar o maior número possível de membros do PCC, em um esforço para restaurar a estabilidade e impedir expansão da quadrilha (LARKINS, 2021).

Infelizmente, essa estratégia teve o efeito contrário, ou seja, apenas fortaleceu a posição da quadrilha. Isso pode ser observado no decorrer da expansão do PCC nos estados do Paraná e Mato Grosso do Sul. A crescente onda de violência gerada pela gangue fez com que as autoridades de ambos os estados prendessem cada vez mais membros do sindicato da morte. Isso permitiu que o Primeiro Comando da Capital conquistasse uma posição dominante nas prisões dos estados do Paraná e Mato Grosso do Sul, assegurasse o monopólio dos mercados criminosos locais e assumisse o controle das lucrativas rotas de drogas por esses estados que ligavam o Paraguai ao Brasil (COUTINHO, 2019). É importante destacar que, entre 2012 e 2016, o Primeiro Comando da Capital iniciou suas operações no Paraguai, tornando-se uma Organização Criminal Transnacional (TCO). Além disso, para aumentar influência no Paraguai, o PCC utilizou as mesmas estratégias que lhe permitiram expandir rapidamente primeiro no estado de São Paulo e depois em outros estados brasileiros (INSIGHT CRIME, 2020).

Atualmente, o Primeiro Comando da Capital tem mais de 32.000 membros em 26 estados e no Distrito Federal do Brasil, a grande maioria dos quais está na prisão, e centenas de milhares de criminosos afiliados ou colaborando com a quadrilha PCC principalmente no narconegócio. O sindicato da morte do PCC é poderoso o suficiente para influenciar os resultados das eleições para governadores de estados individuais, entre outras coisas, financiando as campanhas de candidatos vinculados ao PCC, bem como controlando totalmente os mercados criminosos locais, combatendo organizações criminosas rivais e corruptores dos serviços de segurança (INSIGHT CRIME, 2020).

Além disso, gera apoio popular nas favelas que controla, substituindo o Estado, por exemplo, fornecendo assistência básica e proporcionando uma aparente sensação de segurança. Por exemplo, a quadrilha do PCC cria tribunais especiais nas favelas sob seu controle para mediar todos os tipos de conflitos de negócios a interpessoais, que funciona como um sistema de justiça improvisado. Fora tal, o Primeiro Comando da Capital controla a maior parte das rotas de drogas da Bolívia e Paraguai para o Brasil (COUTINHO, 2019).

Aqui, um bom exemplo é a rota da cocaína caipira que vai da Bolívia através do Paraguai até o porto brasileiro de Santos, de onde a pichicata entra na África, Europa e Ásia por mar. O PCC tem posição dominante em oito estados estratégicos para o narconegócio: São Paulo, Paraná e Mato Grosso do Sul (fronteira com o Paraguai), Acre (fronteira com o Peru), Roraima (fronteira com a Venezuela) e Piauí, Alagoas e Sergipe (acesso ao Oceano Atlântico). Além disso, o Primeiro Comando da Capital tem influência

no Peru, Colômbia e Venezuela, permitindo-lhe vender cocaína no Brasil e atuar como atacadista de outras organizações criminosas. Em frente, o Comando Vermelho. Essa quadrilha foi formada em 1971 no presídio de segurança máxima Cândido Mendes, na Ilha Grande, a poucas horas da cidade do Rio de Janeiro, como resultado de uma aliança entre os internos do Bloco B, ou criminosos associados a roubos e furtos a bancos, e os guerrilheiros de esquerda MR-8 e Aliança Libertadora Nacional (ALN) (LARKINS, 2021; BENJAMIN, 2016).

Inicialmente, um grupo, modelado na estrutura de uma unidade de milícia guerrilheira chamada Falange Vermelha, foi formado para proteger seus integrantes da violência e represálias por guardas prisionais e outras quadrilhas prisionais, prestar assistência necessária e apoiar o planejamento, executando fugas do presídio Cândido Mendes. Os integrantes da Falange Vermelha começaram a criar estruturas de cunho político para lutar pelos direitos dos presos contratando advogados para representá-los, para garantir a melhoria das condições do presídio e também para mediar as negociações entre os presos e a direção penitenciária (LARKINS, 2021; BENJAMIN, 2016).

Além disso, mobilizaram os presos para criar estruturas que lhes permitissem lutar por seus direitos e empoderá-los. A compreensão desses dois grupos díspares de presos também foi facilitada por sua vida comum como prisioneiros da LSN confinados em celas lotadas quase o tempo todo. Note-se que se não fosse o artigo 27º da Lei de Segurança Nacional (LSN) de 1969, promulgada pela junta militar para combater o aumento do número de assaltos a bancos armados por opositores da ditadura, teria sido virtualmente impossível para guerrilheiros se juntarem a criminosos comuns em prisões de segurança máxima (LARKINS, 2021; BENJAMIN, 2016).A ideologia do Comando Vermelho implantada pela guerrilha, baseada na luta em nome da justiça social, inicialmente não conquistou muitos adeptos, mas à medida que a quadrilha CV crescesse, isso mudaria. A primeira grande operação organizada pelo Comando Vermelho foi o assassinato dos líderes de uma quadrilha rival em 1979, o que permitiu aos membros do CV assumir o controle da penitenciária Cândido Mendes e infiltrar alguns membros nas favelas do Rio de Janeiro (COUTINHO, 2019).

Nesse sentido, os membros do Comando Vermelho introduziram um código comum de regras prisionais, chamado de estilo de comportamento, que foi concebido para: a) manter disciplina e lealdade férrea entre os membros, entre outras coisas, com pena de morte para homicídio, roubo, agressão ou estupro de companheiros de prisão e por colaborar com a polícia, guardas prisionais (alcaguetar) ou ingressar em outra

quadrilha; b) unir membros do CV em torno de objetivos comuns, como melhorar as condições prisionais, organizar fugas, combater abusos e repressão; c) reduzir o nível de violência e dar ao Comando Vermelho o monopólio de seu uso; e d) garantir certa autonomia aos membros individuais, permitindo-lhes perseguir seus próprios micro interesses (INSIGHT CRIME, 2021). Esses princípios foram rapidamente adotados no presídio Cândido Mendes e em presídios posteriores para onde foram enviados membros do Comando Vermelho no Rio de Janeiro, gerando apoio à quadrilha. Membros de gangues em geral começaram a cometer sequestros por resgate, roubos de casas e assaltos a bancos para apoiar financeiramente os presos. Essa assistência não foi voluntária, mas forçada pela intimidação dos membros do Comando Vermelho localizados nas prisões do Rio de Janeiro (INSIGHT CRIME, 2020).

Os membros de gangues em geral deveriam viver com a crença de que, se não entregassem dinheiro regularmente às prisões controladas pelo CV como forma de taxa de adesão e fossem recapturados pelas forças de segurança, seriam torturados e posteriormente assassinados como sendo potenciais traidores. Essa política de terror provou ser extremamente eficaz, permitindo que o CV fortalecesse sua posição e controle nas prisões corrompendo guardas, policiais e membros do judiciário (INSIGHT CRIME, 2020). Ao mesmo tempo, com as primeiras fugas bem-sucedidas dos membros de gangues das prisões no início dos anos 1980, o Comando Vermelho começou a tomar os mercados criminosos locais, usando terror e violência contra rivais e moradores locais. Vendo a eficácia, o grau de organização e a força da quadrilha, alguns criminosos locais decidiram se juntar ao Comando Vermelho, na esperança de patrocínio se fossem presos, e aumentar sua própria renda criminal (LARKINS, 2021).

A expansão rápida da cocaína na década de 1980 fez com que cartéis de drogas colombianos (Medellín e Cali) e guerrilhas (FARC, ELN) buscassem novos mercados para a substância. O Brasil tornou-se um dos principais países de trânsito da cocaína produzida na Colômbia, Peru e Bolívia para a Europa, incluindo Itália, Holanda, Turquia e Espanha. À medida que o CV continuava a crescer, uma segunda facção de líderes reunidos em torno de uma facção de traficantes de drogas brasileiros, conhecido como o segundo grupo dirigente, surgiu em uma das prisões para engajar a quadrilha totalmente no narconegócio (INSIGHT CRIME, 2021).

Com a facção fundadora, formada principalmente por assaltantes de banco, fora do poder, o CV se envolveu no narconegócio de contrabando, distribuição e tráfico primeiro de maconha e depois da mais lucrativa cocaína. Os líderes do Comando

Vermelho da facção dos narcotraficantes se dedicaram à tarefa de monopolizar todo o mercado de drogas no Rio de Janeiro e exterminar os narco-independentes. Isso faria do Comando Vermelho o único varejista e, portanto, um parceiro adequado para os cartéis de Cali e Medellín. Em 1984, o Comando Vermelho ganhou vantagem exterminando ou absorvendo outros grupos criminosos. No final de 1985, a quadrilha já controlava 70% do mercado de drogas nas favelas do Rio de Janeiro (INSIGHT CRIME, 2020). Cabe destacar que o Comando Vermelho conseguiu estabelecer cooperação com o cartel de Cali e, posteriormente, por meio dos esforços de um dos líderes do CV, Luiz Fernando da Costa "Fernandinho Beira-Mar", com a guerrilha das FARC. Além disso, graças às operações de Fernandinho Beira-Mar, o CV começou a se expandir para outros estados brasileiros e conseguiu controlar uma das rotas de contrabando do Paraguai para o Brasil nos anos 2000 (LARKINS, 2021).

A quadrilha CV estabeleceu sua própria base nas favelas do Rio de Janeiro, entre outras coisas, explorando as divisões raciais entre afro-brasileiros perseguidos e elites brancas, antagonizando moradores de favelas, que não eram considerados moradores legítimos, com a classe média. Os bandidos começaram a substituir as instituições estatais ausentes, que não tinham interesse no destino dos moradores dos assentamentos marginais, criando uma política de boa vizinhança, ou vizinhança, que é a reciprocidade forçada, baseada em parte na lei do morro ou lei do morro e os princípios incorporados no código prisional do estilo de comportamento (LARKINS, 2021; BENJAMIN, 2016).

O Comando Vermelho proporcionou uma fictícia sensação de segurança e justiça, por exemplo, ao combater crimes comuns (furtos, arrombamentos, roubos, estupros) em troca da cooperação ou silêncio dos moradores no contexto do narconegócio. Além disso, organizou festivais e concertos, concedeu empréstimos para habitação e carros, financiou material escolar para crianças, medicamentos e funerais ou distribuiu alimentos aos mais pobres. Dessa forma, os narcotraficantes associados ao CV garantiam aos moradores que o 'respeitavam' que não só não precisavam temer ataques de membros de gangues, mas que podiam realmente recorrer à ajuda da gangue, diferenciando-se da velha guarda do narcotráfico (BENJAMIN, 2016).

Essa política aplicada nas favelas do Rio de Janeiro pelo Comando Vermelho permitiu que ele ganhasse legitimidade e aceitação de suas ações por parte dos moradores de bairros marginais, atraísse novos integrantes e garantisse o crescimento do narconegócio. Naturalmente, haverá algumas pessoas afeiçoadas ou simpatizantes da quadrilha do CV, aquelas que são amigas dos membros do Comando Vermelho, aquelas

de posição neutra e aquelas que são hostis ao CV (INSIGHT CRIME, 2020). Esse nível de confiança dos moradores em relação aos integrantes do Comando Vermelho se deve aos serviços prestados pela quadrilha: proteção, (investigação e punição de crimes como homicídio, furto, roubo, estupro etc.), distribuição de alimentos, medicamentos, dinheiro para os mais pobres, pavimentação de estradas, reforma de instalações esportivas, financiamento de projetos culturais locais, festas de funk proibidão, times de futebol e partidas. Em troca de tudo isso, os moradores da favela da Rocinha reconhecem a autoridade do Comando Vermelho, se comprometem a ajudar os membros de gangues com o narconegócio (vendendo drogas, escondendo-as ou armas em suas próprias casas), guardando a ordem na favela e permanecendo em silêncio em relação à polícia ou rivais. Todas estas atividades são ampliadas pela troca de informações no CV (LARKINS, 2021; BENJAMIN, 2016). A ocupação das favelas foi um movimento estratégico por parte do CV porque elas tinham locais-chave para o tráfico de drogas, incluindo perto ou nas imediações das principais vias de acesso à cidade e boas vias de transporte para os bairros ricos do Rio de Janeiro. Além disso, as favelas não apareciam nos mapas oficiais da cidade, o que as tornava ideais para os gângsteres se defenderem dos rivais e evitarem ser presos pela polícia. Para garantir sua impunidade, o CV corrompeu departamentos de polícia oferecendo subornos diários, semanais ou mensais em troca dos quais as forças de segurança fariam vista grossa às atividades da quadrilha, reduziram o nível de repressão ou informariam membros do CV sobre patrulhas planejadas nas favelas. Por exemplo, em 1997, a polícia recebia 3.000 reais por dia de traficantes na favela da Rocinha. Ao mesmo tempo, o CV reagiu rapidamente às prisões e assassinatos de seus membros organizando emboscadas em patrulhas policiais, atacando o transporte público e forçando o fechamento de comércios e lojas locais (INSIGHT CRIME, 2020). Essas duas principais facções atualmente estão em praticamente todos os presídios brasileiros, em diferentes proporções e grande parte dos comandantes e chefes estão sobre o escopo da execução penal. Para tanto, agregam inúmeras metodologias diferentes para fundamentar a comunicação, sendo uma delas a criptografia, vista em frente.

3.3 Sistema de Inteligência Penitenciária

A inteligência criminal tem um claro caráter preventivo, fornece “conhecimento” para antecipar e permitir às autoridades neutralizar ou dissuadir as ameaças, riscos e

conflitos ligados ao crime organizado. Seu objetivo específico é alertar sobre atividades criminosas antes que elas ocorram. Ressalte-se que a inteligência criminal nada mais é do que um tipo (tipologia) de inteligência útil para obter, avaliar e interpretar informações e divulgar a inteligência necessária para proteger e promover interesses nacionais de qualquer natureza (políticos, comerciais, empresariais), contra o crime organizado, a fim de prevenir, detectar e permitir a neutralização das atividades, grupos ou indivíduos criminosos que, por natureza e magnitude, consequências previsíveis, perigo ou modalidades, ponham em risco, ameacem ou violem a ordem constitucional, direitos e liberdades (ROBERTO, 2011).

Da mesma forma, sua utilidade resulta em sua utilização como elemento de análise do sucesso das políticas públicas e das decisões adotadas no enfrentamento ao crime organizado (GONÇALVES, 2003). Alocar capacidades de inteligência para realizar análises sobre a gestão pública do Estado e fortalecimento institucional, a fim de vislumbrar com a devida antecipação como certas decisões sobre a gestão do público (recursos, bens e serviços) permitem ou facilitam a operação e o funcionamento de organizações fora da lei, de forma a identificar as implicações das decisões adotadas e dos esquemas preventivos para evitar o fortalecimento involuntário do crime organizado. Ao circunscrever a análise ao ambiente prisional, é imprescindível destacar o fato de que a inteligência criminal, por definição, não se arroga a uma entidade particular, mas, dependendo de circunstâncias de vários tipos – administrativas e políticas – principalmente ou de natureza circunstancial, esse trabalho pode ser realizado tanto em serviços de inteligência, como em unidades policiais, alfandegárias, penitenciárias e até mesmo em organizações militares. A este respeito, refira-se que a transversalidade da criminalidade organizada significa que a atribuição de competência a um ou outro serviço em virtude da sua competência na esfera interna ou externa da segurança, nos casos de modelos com pluralidade de serviços, é absolutamente sem sentido (GONÇALVES, 2003).

Diante da transnacionalização do crime organizado, a tradicional diferenciação entre segurança interna e externa perde sua funcionalidade, borrando vertiginosamente as fronteiras quando nos referimos às atividades realizadas por organizações do crime organizado, para as quais a inteligência criminal opera indistintamente nos dois polos da segurança. No entanto, com base na distribuição teórica dos poderes de segurança entre os diferentes atores do Estado, a segurança interna tem tradicionalmente recaído sobre os

Corpos e Forças Policiais, sendo as Forças Armadas responsáveis pela segurança externa (ROBERTO, 2011).

A teoria nem sempre se ajusta à realidade, especialmente considerando que alguns estados optaram, motivados por diversas causas, por recorrer às Forças Armadas para manter, se não recuperar, o controle de suas instituições penitenciárias, atribuindo-lhes todo tipo de poderes associados à gestão das prisões, sem um mandato claro quanto aos limites de poderes e temporários do mesmo (GONÇALVES, 2003). Atribuição de poderes que, somados à participação dos militares no combate ao narcotráfico e a recente assunção de tarefas na prestação de segurança cidadã, tem levado à imersão total das Forças Armadas na inteligência criminal. Resumidamente, nota-se que a exploração da inteligência criminal na esfera penitenciária difere diretamente do desenvolvimento das capacidades de inteligência penitenciária, embora possam compartilhar fontes de obtenção e aproveitar as mesmas informações, metodologias de análise e objetivos, isso sim, sob diferentes perspectivas (GONÇALVES, 2003).

Ambos os tipos de inteligência não deixam de constituir meras subcategorias de inteligência (tipologias), em virtude do objeto de análise (inteligência criminal) ou da área de trabalho (sistema penitenciário). Assim, a inteligência criminal se limitaria à continuidade do combate ao fenômeno do crime organizado dentro do espaço penitenciário, supondo que haja vínculos dentro e fora dele (não faz sentido isolar a inteligência criminal com repercussão dentro da prisão), nem a administração penitenciária, de toda a inteligência criminal elaborada pelo resto da comunidade de inteligência, seja de origem militar, policial, econômica, financeira, aduaneira ou de serviços de inteligência. Por seu lado, a inteligência prisional implicaria tudo o que se relacionasse com gestão e proteção direta ou indireta do sistema prisional (detentos, infraestrutura, classificação de presos, estratégias institucionais, política prisional) e com a segurança de seus integrantes (funcionários), tanto dentro da instituição quanto fora dela, apoiando iniciativas de segurança pública (GONÇALVES, 2003).

A partir dessa breve diferenciação conceitual, mas necessária, abre-se todo um debate doutrinário em relação ao modelo praticamente inexistente ou subdesenvolvido de inteligência prisional e exploração da inteligência criminal, com exceções como Israel (Serviço Prisional de Israel), Brasil (Inteligência de Segurança Penitenciária –ISPEN–) ou dos Estados Unidos, este último se concentrava quase exclusivamente nas gangues (Gangue da Inteligência) que predominavam em seus presídios. Nessa linha, as iniciativas antiterroristas desenvolvidas nos sistemas penitenciários (inteligência antiterrorista) não

são objeto de reflexão (LACERDA, 2003; GONÇALVES, 2003). A questão está em identificar a opção mais vantajosa, criando um centro de inteligência prisional (também com competências em inteligência criminal dentro do sistema prisional) com unidades ou departamentos de inteligência em cada centro, ou outra arquitetura de inteligência, com capacidade para recolher e desenvolver, inteligência tática e estratégica (LACERDA, 2003; GONÇALVES, 2003).

Isto, com o consequente investimento na formação de quadros penitenciários ou de perfis profissionais recém-incorporados. E o mais difícil ainda, levando em conta as respectivas idiossincrasias (comportamento peculiar) dos diferentes modelos de sistemas prisionais e serviços de inteligência. E, logicamente, que essa inteligência gerada seja compartilhada dentro de toda a comunidade de inteligência (LACERDA, 2003). Um dos meios da inteligência policial em penitenciárias hoje em dia é utilizar o uso de mensagens criptografadas para evitar a comunicação entre as organizações criminosas. Mas, para tanto, é importante compreender como ocorre o funcionamento desta área no cenário do Brasil, fundamento desta pesquisa, cuja metodologia se apresenta no próximo capítulo observado, logo em frente.

CAPITULO IV: ESTUDO DE CASO

Nesse capítulo, são discutidos os resultados relacionados com o questionário aplicado aos profissionais da área, atuantes nas diversas unidades prisionais do Brasil, obtendo informações de 18 unidades federativas diferentes.

Assim esta análise se divide em três dimensões para além da metodologia científica: a primeira trabalha o perfil sociodemográfico da amostra; a segunda elenca as características das instituições em que trabalham e do perfil dos presidiários. A terceira amostra trabalha com as características de infraestrutura e conhecimento de criptografia. Discussões são desenvolvidas ao longo dos dados que foram colhidos, através de autores.

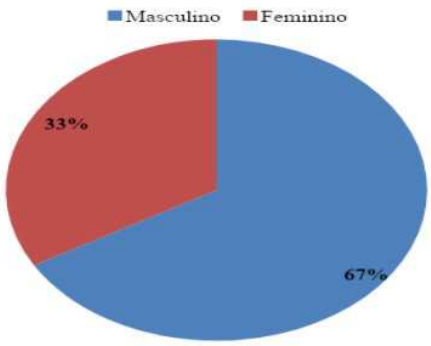
4.1 Metodologia

Foi aplicada uma pesquisa eletrônica, qualitativa, com funcionários que trabalham dentro do sistema penitenciário brasileiro. A pesquisa foi realizada no mês de agosto de 2022 e obteve um total de 18 respondentes.

4.2 Resultados Iniciais: Perfil da Amostra

Nessa seção de "Perfil da Amostra" são evidenciadas as características de gênero, idade e profissão exercida pelos profissionais que responderam esta pesquisa. Isto posto, o Gráfico 1 apresenta os resultados de gênero.

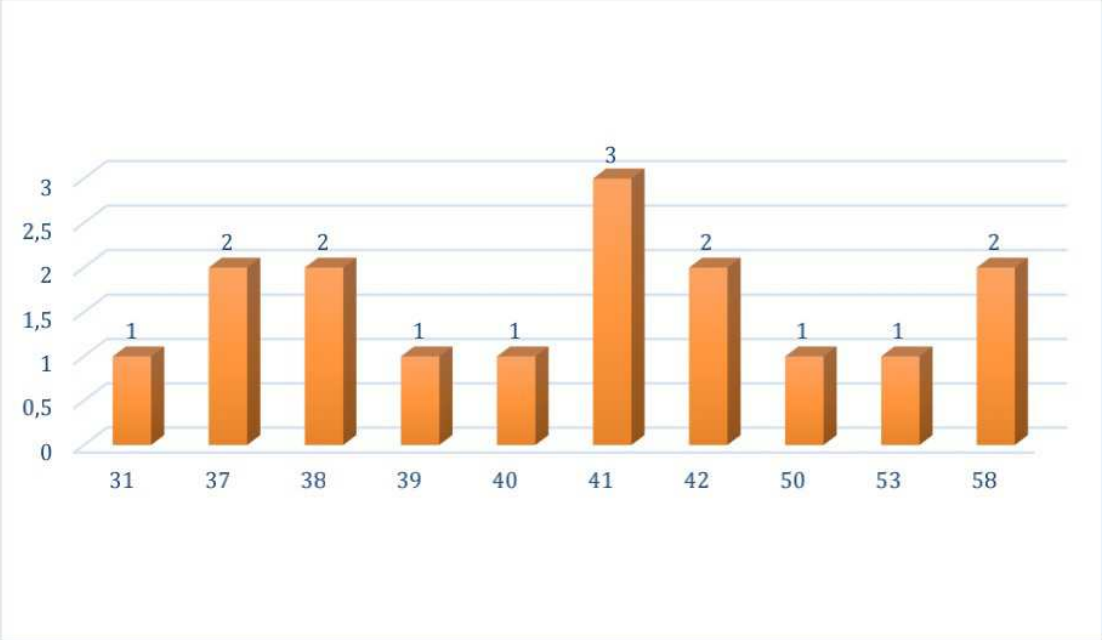
Gráfico 1: Gênero da Amostra



Fonte: Elaborado pela Autora (2022)

Do total de 18 respondentes, portanto, 33% foram do gênero feminino (n=6) enquanto 67% correspondem ao gênero masculino (n=12). Não foi identificada nenhuma resposta que não se enquadrasse dentro destes dois gêneros, embora aberta a possibilidade no questionário. Posto isto, a idade da amostra é evidenciada em frente.

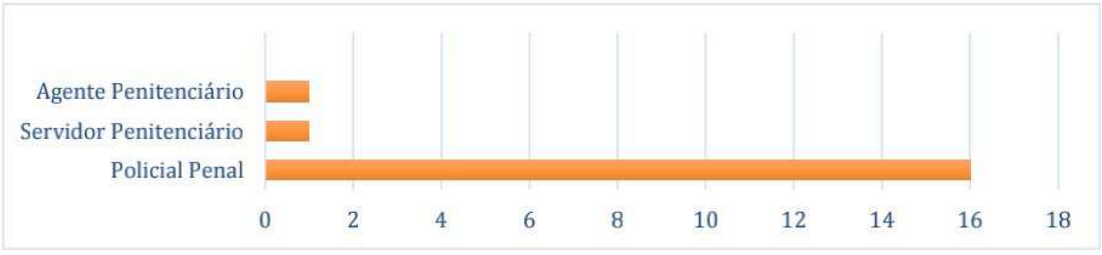
Gráfico 2: Idade da Amostra



Fonte: Elaborado pelo Autora (2022)

O maior grupo de idade foi de 41 anos (n=3), o que representa 16%. Este grupo foi seguido das idades de 58, 42, 37 e 38 anos, com resultados iguais de 11% (n=2). As demais idades resultaram em 5% (n=1) da amostra. Em frente, são apresentados os profissionais e os cargos exercidos pelos profissionais nas unidades em que atuam.

Gráfico 3: Exercício de Profissão da Amostra



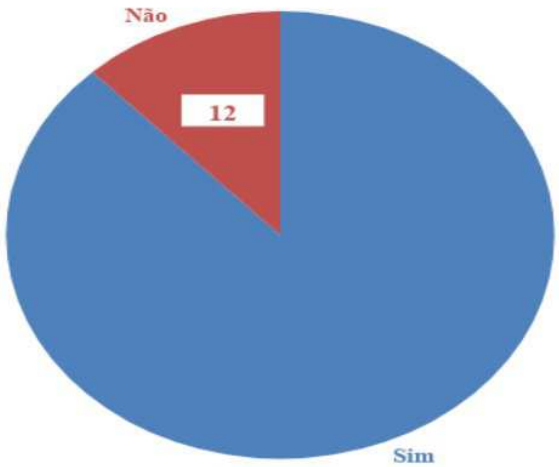
Fonte: Elaborado pela Autora (2022)

O maior grupo da amostra, com representação de 88,8% dos respondentes, é de policiais, que atual na área penal. Já os demais grupos, com respectiva participação de 5% cada um destes, são relacionadas com agentes penitenciários propriamente ditos e também um profissional servidor, que exerce a profissão como contratado pelo Estado. As bases profissionais, portanto, trazer significância na prática para esta pesquisa, haja vista que os pesquisados atuam diretamente no sistema prisional com cargos estratégicos na área. Determinadas essas noções sociodemográficas, parte-se ao perfil das instituições, em frente.

4.3 Perfil das Instituições e dos Encarcerados

A amostra observada resultou em significativa variância quando se fala na quantidade de encarcerados nas instituições. Apenas dois grupos foram citados mais de uma vez: o primeiro é de 45 presidiários na instituição (n=3) e o segundo é de 800 (n=2). Todos as demais respostas assumem que os profissionais trabalham em instituições com diferentes capacidades bem como quantidade de encarcerados, sendo que os resultados foram 3000, 320, 60000, 400, 180, 500, 600, 1450, 200, 450, 890, 308 e, inclusive, uma resposta afirmou que não apresenta nenhuma categoria de encarcerados. Delimitado o perfil das instituições, questionou-se sobre a existência de comunidade significativa de crime organizado na unidade. As respostas estão apresentadas no Gráfico 4, em frente.

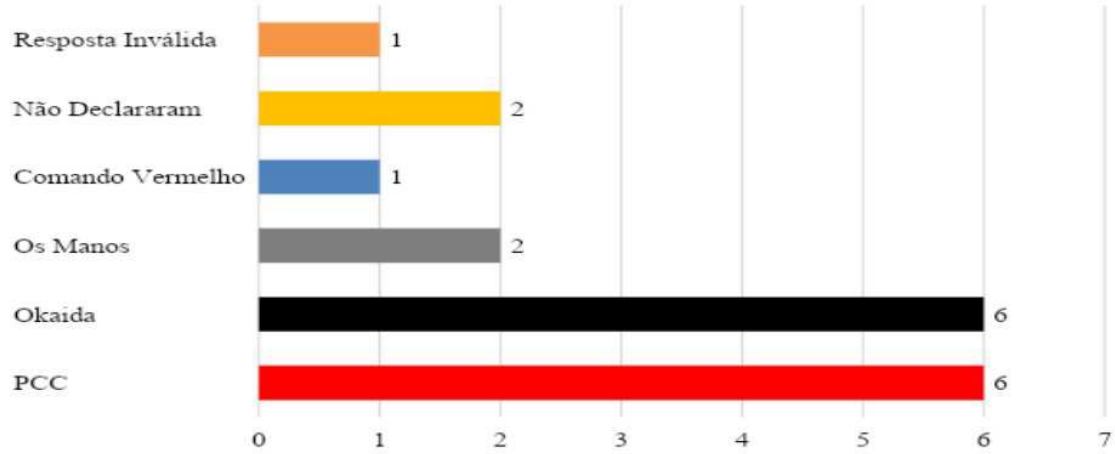
Gráfico 4: Comunidade significativa de crime organizado na unidade prisional.



Fonte: Elaborado pela Autora (2022)

88% dos respondentes, (n=16) selecionaram a opção "sim", afirmando que existe presença de organização criminosa relevante na unidade em que atual. Apenas 12% (n=2) afirmaram que a unidade não conta com organizações de grande atividade. Nesse sentido, aproveitou-se para questionar quais os grupos mais observados. A resposta dos pesquisados se encontra no Gráfico 5, elencado em frente.

Gráfico 5: Grupos de Maior Relevância



Fonte: Elaborada pela Autora (2022)

Em face do Gráfico 5, Primeiro Comando da Capital (PCC) recebeu o maior número de menções, representando 33,3% da amostra (n=6) juntamente com o Grupo Okaida, em escala estatística. Estes dois grupos foram seguidos pelo "Os Manos", com n = 2, respectivamente, e perfazendo percentual de 12%. 2 respostas afirmaram não saber da existência de grupos.

Além disto, O Comando Vermelho (CV) recebeu uma resposta (5,5%) e uma resposta não se efetivou da maneira planejada à questão. Aqui se faz importante mencionar que os dados se relacionam com os dois principais grupos já mostrados nesta pesquisa, todavia, o "Os Manos", ainda não falado, também apareceu com significativa percepção. Assim, logo em frente, apresentam-se algumas das características desse grupo.

Sendo uma das principais organizações do sul do Brasil, Os Manos surgiu no interior da superlotada Cadeia Pública de Porto Alegre, que hoje é conhecida como Presídio Central, ainda na década de 1980 (PORTO, 2008). Nesse sentido, segundo Bernardi (2017), esta é a "mais antiga entre as organizações das regiões, posicionando-se como uma das principais do Brasil, em dimensão financeira e estrutural.

4.4 Estrutura das Instituições (Penitenciária & Crime)

Em relação à estrutura das instituições, o primeiro questionamento realizado foi sobre a utilização de bloqueadores de sinais ou antibloqueio nas penitenciárias. A resposta foi negativa para o controle e também combate ao crime organizado, haja vista que somente 22% (n=4) dos pesquisados assumiram que a sua unidade apresenta esta tecnologia. Os demais (n=14), os quais representam 78% da amostra, responderam que não há nenhuma tecnologia que auxilia nessa área dentro de sua instituição.

Nesse sentido, para Santos; Tagliaferro (2017), que apresenta:

> Não há somente uma questão de boa vontade ou boa-fé por parte da administração pública em relação à instalação dos respectivos aparelhos bloqueadores de sinal, mas sim toda uma gama de interesses que extrapolam até mesmo os interesses dos Estados e das operadoras, atingindo também o direito de acesso à comunicação, seja ela pela via telefônica ou informática, das populações que residem em regiões que são periféricas, porém, próximas aos locais onde esse sinal estaria prejudicado (SANTOS; TAGLIAFERRO, 2017, p. 10)

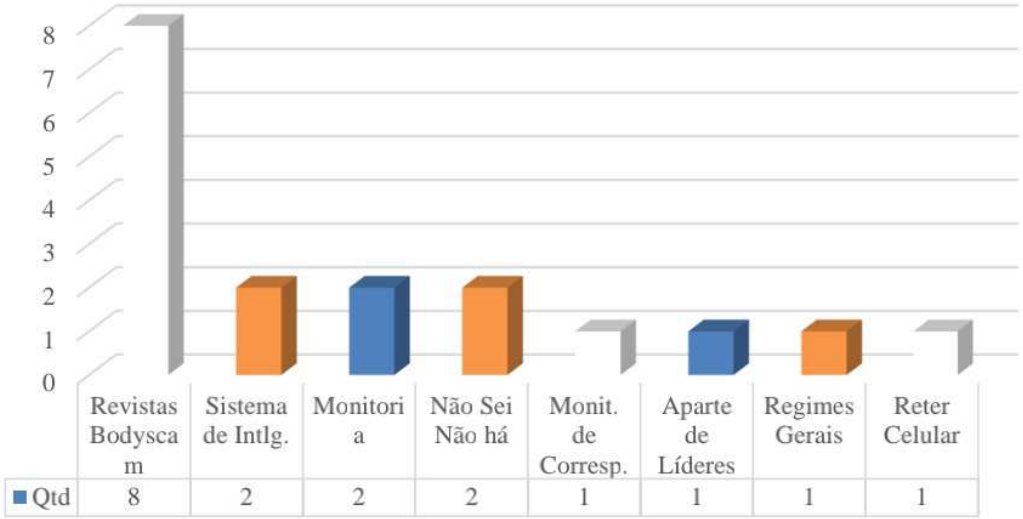
Na compreensão desses autores, o problema de falta de tecnologia de antibloqueio ou de bloqueadores de sinal é relacionado não somente pela sistemática financeira-econômica, mas também pelo institucional privado, em que as empresas de telecomunicação têm tutelado o direito de comunicação e liberdade e, ao mesmo tempo, esse mesmo direito acaba por agravar a possibilitar de ter bloqueadores pela existência de interferência na comunicação da região onde se encontra a instituição.

Nesse sentido, é oportuno destacar que a própria Lei n. 12.850/13 (de ação e organização criminosa no Brasil) prevê a instalação de bloqueadores de sinal telefônico nos presídios ou em centros penitenciários, mas, esta não é a realidade observada pela maior parte das instituições do Brasil, e isto se prevalece pela inexistência tanto de prazo quanto de previsão de inclusão dessas tecnologias no serviço penal brasileiro.

Baseando-se nessa lei (12.850), fica perceptível que a implementação de bloqueadores é um mecanismo obrigatório, mas não há qualquer regularidade expressiva, a considerar todas as respostas apresentadas nessa seção. A este fundamento, o Projeto de Lei 32/2018, que tem por objetivo "a utilização de recursos do Fundo Penitenciário Nacional para a instalação de bloqueadores de sinais de telecomunicação para telefones celulares e aparelhos análogos em estabelecimentos penitenciários no prazo de 180 dias", aprovado pelo Senado, agora passa em votação na Câmara dos Deputados e, se aprovado,

pode vir a mudar a realidade observada pela amostra selecionada nesta pesquisa. Isto posto, fica evidente que os bloqueadores não são ativos operacionais ainda em utilização no Brasil. Com isto, aproveitou-se também para questionar os pesquisados sobre as outras possíveis tecnologias ou artefatos que são utilizados para combater o crime organizado e a troca de informações. As respostas foram variadas, mas, em suma, comportam revistas e/ou bodyscam, como se vê no Gráfico 6, em frete.

Gráfico 6: Alternativas de Segurança nas Instituições.



Fonte: Elaborado pela Autora (2022)

Como notado no Gráfico 6, 45% da amostra relatou que as operações de revista ou de *bodyscam* é a principal forma de evitar a transmissão de informação e a movimentação de ações do crime organizado. Regimes gerais (5,55%, n=1) também é uma forma que considera esta análise e, ao mesmo tempo, a monitoria ou monitoramento (11%, n=2) também se respalda em condutas relacionadas com estas. Assim, pode-se compreender que 61,1% da amostra assume que a revista pessoal é o principal método de redução do crime organizado.

Em segundo lugar, os sistemas de inteligência também foram apontados. Aqui cabe notar que sistemas de inteligência não estão diretamente relacionados com a vertente tecnológica, mas com a dimensão estratégica da polícia. As respostas não assumiram quais os sistemas de inteligências, mas, como relatado por Oliveira (2019), sistemas recorrentes desenvolvidos por penitenciárias brasileiras são os SISBIN, DNIPEN, ABIN e PNI, que apresentam traços e ações estratégicas para reconhecer as metodologias de

comunicação e de linguagem das organizações criminosas (OLIVEIRA, 2019). Esta autoria ainda destaca a importância desses sistemas de inteligência para reduzir a criminalidade que sai de dentro do presídio (onde estão os chefes dessas organizações), como afirmado em frente:

> Não custa lembrar que a grande maioria dos líderes das organizações criminosas encontram-se encarcerados, e é justamente de dentro dos diversos estabelecimentos prisionais em todo o país, que emanam as ordens para as mais variadas ações delituosas, inclusive de afrontamento ao próprio Estado de Direito, restando claro, a partir disso, que as unidades prisionais representam importantes fontes de obtenção de dados e produção de conhecimentos, sendo justamente por isso, que as autoridades de segurança pública deverão valorizar os órgãos e agências de inteligência prisional, viabilizando seu pleno funcionamento e desenvolvimento, buscando a evolução em todos os sentidos, tanto estrutural, como em relação a capacitação dos servidores. De fato, é possível ainda identificar deficiências, especialmente no quesito integração e interoperabilidade, entretanto, resta inegável que a inteligência prisional, a nível nacional, alcançou um patamar diferenciado, evoluindo em vários fatores, prestando um grande serviço à sociedade, representando um instrumento indispensável para a segurança pública do nosso país (OLIVEIRA, 2019, p. 37).

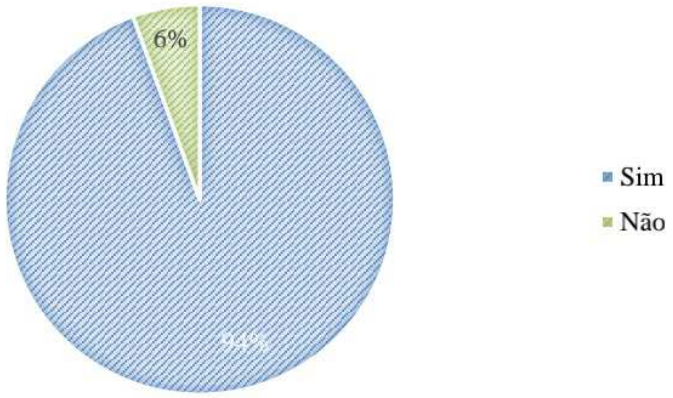
É importante lembrar que os sistemas de inteligência dependem das tecnologias, tais como os meios de averiguar bloqueios de sinais ou interromper ligações bem como rastreá-las. A monitoria de correspondência (n=1) também é uma das aliadas, e foi observada na amostra, em 5,5%. O aparte de líderes (n=1) e a retenção de celulares (n=1) também pode ser utilizada por estes sistemas. Assim, é importante consolidar a inteligência prisional para reduzir a criminalidade nos presídios do Brasil, especialmente considerando o que Oliveira (2019) citou: "a inteligência prisional, a nível nacional, alcançou um patamar diferenciado" (OLIVEIRA, 2019, p. 37). Em frente, às análises de Criptografia.

4.5 Utilização e Identificação Da Criptografia

Previamente a determinação das dimensões da Criptografia encontrada nas organizações, foi realizada uma avaliação sobre o conhecimento e a produção de conhecimento nessa área pela amostra da pesquisa. Assim, o Gráfico 7 apresenta os

resultados auferidos a partir do seguinte questionamento: "Você sabe o que é Criptografia?':

Gráfico 7: Conhecimento Sobre Criptografia



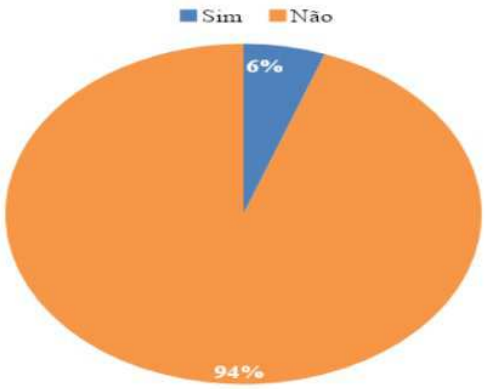
Fonte: Elaborado pela Autora (2022)

A amostra revelou que 94% (n=17) sabe o que é Criptografia. Compreender que tais profissionais sabem do que se trata é fundamental, haja vista que o estudo e reconhecimento de Criptografia é essência para barrar o crime e organizações criminosas no Brasil. Veja-se isto no exposto por Silva (2014, p. 92):

> É possível afirmar que os órgãos de investigação estarão cerceados de implementar técnicas especiais de obtenção de prova, imprescindíveis para apuração de crimes graves como o terrorismo, por exemplo, bem como o desmantelamento de organizações criminosas, razão pela qual é de se reconhecer que a criptografia permanecerá sendo uma ferramenta de comunicação segura para os agentes criminosos no Brasil, contrariando assim a tendência internacional que é de permitir hacking e infiltração virtual, conforme observamos recentemente na Europa, reconhecida por sua legislação protetiva da privacidade, mas não para a criminalidade organizada (SILVA, 2014, p. 92)

Considerando sua importância, os profissionais foram questionados quanto a existência de cursos ou treinamentos relacionados com esta ciência. As suas respostas estão elencadas no Gráfico 8, disponibilizado em frente.

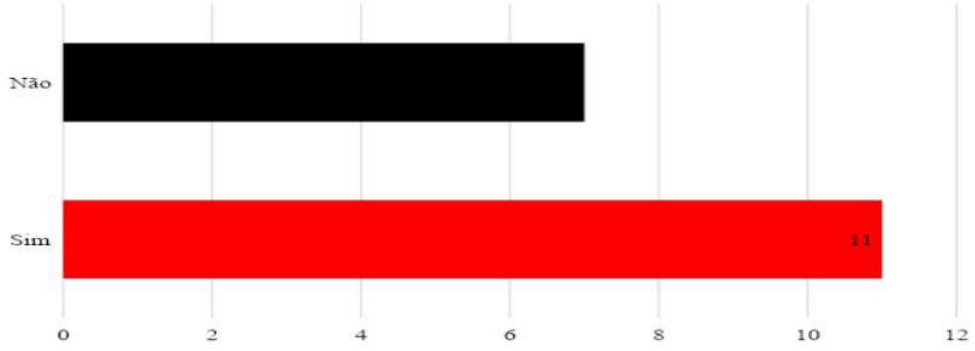
Gráfico 8: Treinamento dos profissionais sobre Criptografia na Unidade Prisional



Fonte: Elaborado pela Autora (2022)

Contrariamente ao conhecimento dos profissionais sobre Criptografia, a amostra relata que não existem cursos de formação direcionados para esta área, o que se mostra como um fator preocupante para, por exemplo, a eficácia dos sistemas de inteligência nessas organizações, que dependem de profissionais capacitados para lidar com os meios de comunicação presentes entre diferentes organizações. Frente a isto, questionou-se sobre os treinamentos que os profissionais participaram dentro ou fora da unidade. A resposta foi a seguinte:

Gráfico 9: Participação em algum treinamento (fora ou dentro da unidade).

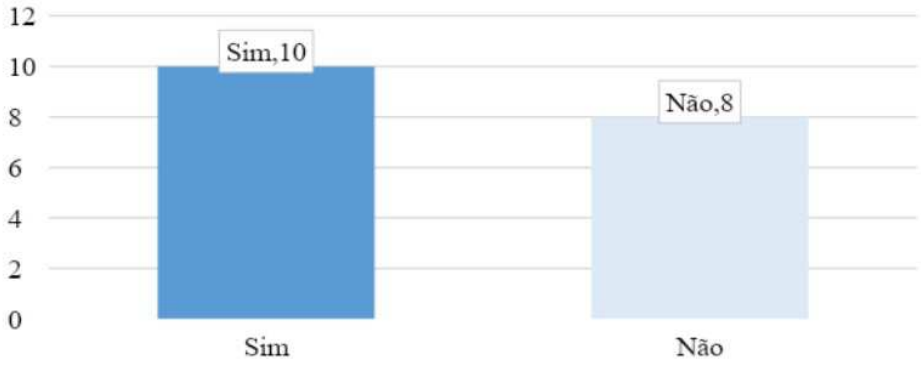


Fonte: Elaborado pela Autora (2022)

Um total de 11 respondentes que relataram ter participado de treinamento relacionado com Criptografia (61,1%). Outros 7 afirmaram que não (38,9%). Este número é expressivo e se relaciona com o fato de que 94% da amostra reconhece a criptografia.

Esse resultado também é alinhado com a identificação de casos pelos profissionais, conforme observado no Gráfico 10, apresentado em frente.

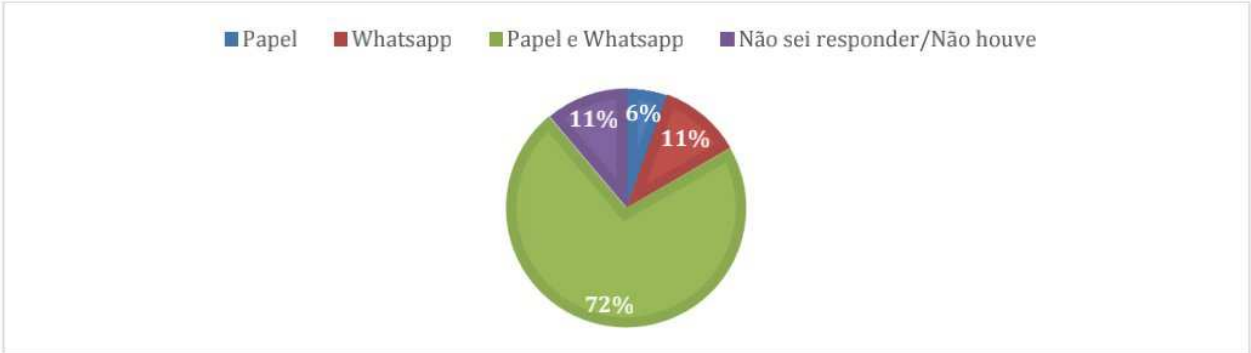
Gráfico 10: Identificação de Mensagens Criptografadas em serviço



Fonte: Elaborado pela Autora (2022)

Um total de55,5% da amostra (n=10) assumiu que já identificou alguma mensagem criptografia em serviço. É importante consolidar a quantidade semestral encontrada, que foi objeto de outro questionamento a amostra. Nesse caso, o maior número de respostas desses indivíduos foi "Até 5", que representou 66,6% dos que afirmaram já ter encontrado. "Entre 5 e 10" casos diagnosticados foi apresentado por 22,2% da amostra (n=4) enquanto apenas 11,1% (n=2) relatou que encontra mais de 10 casos por semestre. Como observado no Gráfico 11, 45,5% dos pesquisados (n=8) assumiu que não identificou nenhuma mensagem que utilizou criptografia nas organizações criminosas. Em relação aos respondentes positivos, o Gráfico 11 elenca quais os meios de troca de mensagens mais evidentes.

Gráfico 11: Meios de Troca de Mensagens Criptografadas



Fonte: Elaborado pela Autora (2022)

Apenas 11,1% (n=2) da amostra não respondeu a este questionamento, o que se alinha com as revisões dos outros questionamentos, advindo dos mesmos pesquisados. Já aqueles que identificaram mensagens criptografadas em sua unidade, os principais meios foram papel (6%), com n=1 e Whatsapp (n=2) somando um total de 11,1%. Mas, principalmente, o uso desses dois artefatos foi relatado em maior escala por todos os pesquisados (72%, n=13).

Isto se alinha com a visão de Silva (2014), que expressa que as organizações criminosas estão se tornando, cada vez mais e com mais frequência, tecnológicas, a ponto de apresentarem mais tecnologias/pesquisas do que os próprios sistemas de informação e inteligência da polícia e da comunidade como um todo. Assim, ações são amplamente necessárias para mitigar todos os riscos assumidos na comunidade.

Dúvida relevante é quanto aos conteúdos que são repassados pelas mensagens. Este foi o último questionamento realizado pelos entrevistados. A Figura 12 apresenta um quadro de funções e mensagens que são repassados de acordo com a amostra, reproduzido em escala de apresentação e expressão estatística.

Figura 12: Principais Conteúdos de Mensagem

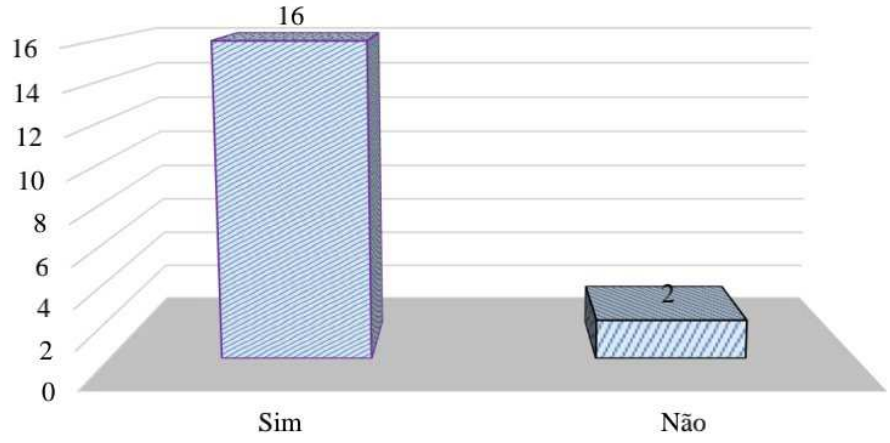
Fonte: Elaborado pela Autora (2022)

Como observado, as principais mensagens se relacionam com a ordem de ação dentre suas múltiplas naturezas, mandados e comércios de drogas ou de realização de crimes. Além disto, foi relatado pela amostra da pesquisa mensagens de negociação, "salve" para chefes ou pessoas de relevância, ordens para compra de celulares ou de drogas, manutenção de crimes ou de sistemas de hierarquia, dentre múltiplos outros. Sobre esta perspectiva, é importante analisar a visão de Cunha (2018):

> Todos os integrantes devem cumprir sem questionamento os "salves", ou seja, ordens emanadas de seus dirigentes; assim, se for dado um "salve geral" para rebeliões nas cadeias, todos os integrantes devem participar das mesmas, sob pena de "julgamento" e execução. O "estatuto" do PCC dispõe ainda sobre lealdade, respeito e solidariedade acima de tudo e cada um recebe dividendos conforme a participação no crime. Estima-se que o PCC conte atualmente com cerca de 10 mil homens engajados e cerca de 90 mil simpatizantes, controlando 90% das cadeias paulistas, através de seu representante mais ativo Marcos Camacho, o Marcola (CUNHA, 2019, p. 28)

É evidente, logo, que o reconhecimento das mensagens é essencial para comprometer o sistema de informação do crime organizado; e, nesse ponto, a Criptografia dificulta as ações e atividades policiais, conforme as respostas da amostra, vista no Gráfico 12, sobre a ação ou não de dificuldade de Criptografia à inteligência policial:

Gráfico 12: "O uso de criptografia dificulta o serviço de inteligência da unidade prisional?



Fonte: Elaborado pela Autora (2022)

Um total de 16 indivíduos (88,8%) responderam que a Criptografia influência as operações e as atividades relacionadas com o diagnóstico e mitigação do crime organizado. Nesse caso, foi questionado as principais características dessa influência. As respostas foram amplas, tais como "*Por se tratar de vários códigos criptografados, se demanda um tempo para se obter os dados e entender a linguagem usada. E sem contar as constantes mudanças de criptografias para tentar burlar as investidas das equipes*".

A demanda e a dificuldade científica, portanto, são fatores significativos. Além disto, outra resposta relevante foi: "*Algum termo ou sigla diferente demora mais para ser decifrada prejudicando a tradução da mensagem. Mas os apenados (principalmente os trabalhadores) revelam ao serem questionados*". Todas estas estão ligadas com a falta de treinamento dos profissionais, em grande maioria. A Figura 13 expressa as principais menções da amostra, em frente.

Figura 13: Principais Conteúdos de Mensagem

Fonte: Elaborado pela Autora (2022)

Com isto, fica evidente que o sistema brasileiro penitenciário ainda apresenta grande dificuldade em barrar a comunicação e a interpretação de mensagens criptografadas dentro dos presídios, mesmo que a lei já estabeleça condutas científicas relacionadas com esta temática. A este sentido, podem ser desenvolvidas algumas conclusões sobre o desenvolvimento deste estudo, as quais estão apresentadas em frente.

Apresentados estes fundamentos, cabe contextualizar ainda notícia recente que saiu sobre o líder do PCC, em que se descobriu o uso de criptografia para avisar sobre a sua fuga. Como exposto pela Jovem Pan (2022), em ligações, percebeu-se que o Plano STJ era um código para orquestrar o sequestro de autoridades e seus familiares do sistema penitenciário. Por último, ainda havia um plano suicida que seria colocado em prática com a tomada de servidor público como refém para que uma rebelião fosse iniciada no presídio. Estes planos foram todos interceptados e descobertos por profissionais. A passagem é significativamente interessante:

> Eu queria um favor do doutor Bruno [membro do PCC fora da prisão], que eu estou pedindo para ele três meses um advogado que cuida de instância superior [planos de fuga]. Eu gostaria muito que, quando ele viesse aqui, ele viesse com a resposta já se o cara vai vir ou não vai, porque daí eu contrato outro. (...). Para STF, STJ [planos de fuga]. Essas coisas, entendeu? (JOVEM PAN, 2022, n. p.).

Fica evidente, portanto, a importância da criptografia para o desempenho penal, em que pese as considerações finais em frente.

CONSIDERAÇÕES FINAIS

A criminalidade parece estar associada diretamente com a história do desenvolvimento da sociedade brasileira. Não por menos, ao longo dos seus mais de 500 anos de construção, milhares de centenas de grupos coletivistas (não somente organizações ligadas às drogas, tráfico e insumos ilícitos) estiveram sobre o poder econômico, financeiro e estrutural por meio de atividades ilícitas. A este caso, a sua comunicação foi fator importante para sua prevalência na história brasileira.

A comunicação é um fator essencial para o desenvolvimento organizacional. A própria literatura de marketing assimila a importância de reduzir os ruídos operacionais para que se tenha o máximo aproveitamento das ações e atividades desenvolvidas. A este sentido, parece que o crime organizado também segue estas premissas fundamentais.

Nessa pesquisa, consolidou-se algumas das principais organizações do Brasil. Em fato, não se pode deixar de falar do Primeiro Comando da Capital (PCC) e do Comando Vermelho (CM) como os grandes protagonistas. Instaurados de norte a sul do país, suas operações reduzem significativamente os recursos financeiro-econômicos do Brasil, além de ratificar problemas com desenvolvimento social e índices de criminalidade. Todos estes, juntos, reduzem a visão da qualidade de vida do brasileiro.

Diversos são os meios e metodologias que estes se comunicam. Fundamentalmente, o uso da Criptografia parece ser um dos mais usuais por garantir o maior sigilo e segurança das informações que são repassados por estes grupos e, ao mesmo tempo, por reduzir possibilidade de ação do Estado e do poder de polícia para combater o crime organizado. Isto ficou evidente ao longo da pesquisa *in loco* realizada com profissionais, em que a máxima destes afirmou já ter algum contato com mensagens criptografadas.

Em suma, os meios alteraram ao longo do tempo. Por exemplo, o que antes era feito por meio de mensagens subliminares e criptografadas em papéis, nos dias atuais passou para meios de comunicação eletrônica e dialetos específicos, como o caso relatado recente da fuga prevista para o chefe central do PCC. A amostra relatou que os recursos tecnológicos mais utilizados são o whatsapp (por apresentar criptografia direta), uso de aparelhos telefônicos e mensagens por meios diversificados (eletrônicos e reais), que buscam reduzir os ruídos de comunicação e ampliar as possibilidades da mensagem emitida chegar ao destino. Esta pesquisa identificou a Criptografia como um pilar

importante para consolidar a segurança pública no Brasil, em que pese o crime organizado estar diretamente lastreado por meio de tecnologias desenvolvidas e, inclusive, internacionais.

Ao contraponto, a educação dos profissionais não parece seguir o mesmo caminho de inovação e resultados. Poucos são os cursos oferecidos nas unidades e, em grande parte, são os próprios profissionais, por conta própria, que buscam atividades extra organizacionais para consolidar conhecimento sobre criptografia. Isto infere em alterações financeiras, que pode não ser viável para grande parte dos profissionais de segurança.

Aliado a isto, a estrutura das unidades também não está adequada e atualizada com as necessidades do sistema de segurança. Em grande parte, não há sinalizados nem bloqueadores de sinal e o acesso a utensílios dentro do presídio, embora muito se busque combater, ainda é facilitado por meio de corrupção e outros fatores. Todos estes itens resultam em comunicação eficaz do crime organizado por meio de Criptografia, pois (a) não há profissionais suficientes e nem capacitados para combater e (b) não há estrutura que mitigue riscos de maneira eficaz para combater o crime organizado.

Com isto, ficam-se recomendações quanto às adequações a lei federal que determina a atualização de presídios brasileiros em busca de evidenciar maior ruído dentro dos meios de comunicação do crime organizado. Somente assim será possível iniciar uma conduta alinhada para combater este tipo de crime no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, E. J. **Criptografia**: **dos rudimentos à atualidade**. 6 p. Dissertação (Mestrado em Matemática). Pós-graduação em Matemática PROFMAT da UNIRIO, 2018.

BARCZAK, C. L. **A Indecifrável Enigma**. São Paulo. Clube de Autores. 2014.

BECCARIA, C. **Dos delitos e das penas. São Paulo**: Editora Martin, 2002.

BENJAMIN, J. ***Inside Out: The Challenge of Prison-Based Criminal Organizations***, part of the Brookings seminar, "Reconstituting Local Orders". Washington DC: Brooking Insti- tution Press, 2016.

COSTA, D. D**. A Matemática e os Códigos Secretos**: Uma Introdução à Criptografia. 78 p. Tese (Programa de Mestrado Profissional em Matemática). Universidade Estadual de Maringá, 2014.

COSTA, F.; FIGUEIREDO, L. M. (Orgs). **Introdução à Criptografia**. Fundação CECIERJ: Consórcio CEDERJ. Rio de Janeiro: UFF / CEP – EB, 2010.

COUTINHO, Leonardo. "**The Evolution of the Most Lethal Criminal Organization in Brazil – the PCC"**. *PRISM*, vol. 8, no. 1, 2019, pp. 56-67.

ENCINAS, L. H. **La criptografia**. CSIC: México, 2016.

GONÇALVES, Joanisval Brito. **A atividade de inteligência no combate ao crime organizado: o caso do Brasil.** Santiago, Chile, 2003.

LACERDA, Mônica Maria Ferreira. Processo cíclico e análise de inteligência Policial. In: BRANDÃO, Priscila; CEPIK, Marco. (Org). **Inteligência de Segurança Pública: teoria e prática no controle da criminalidade.** Niterói: Impetus, 2013.

LARKINS, Erika Robb. ***The Spectacular Favela****: Violence in Modern Brazil*. Oakland: University of California Press, 2021.

LUND, P**. O Livro dos Códigos**. Berkeley e Los Angeles, Califórnia: University of California Press, 2019. ISBN 9780520260139.

MACHADO, N. O; GUIMARÃES, I. S. A Realidade do Sistema Prisional Brasileiro e o Princípio da Dignidade da Pessoa Humana. Revista Eletrônica de Iniciação Científica. Itajaí. **Centro de Ciências Sociais e Jurídicas da UNIVALI**. v. 5, n.1, p. 566-581, 1º Trimestre de 2014

MINHOTO, L. D. **Privatização de presídios e criminalidade**: A Gestão da Violência no Capitalismo Global. São Paulo: Max Limonad, 2021.

OLIVEIRA, R. C. **Inteligência Penitenciária: Relevância e contribuições para a segurança pública**. Monografia, Curso de Pós-Graduação Latu Sensu, em Inteligência de Segurança. Universidade do Sul de Santa Catarina, 2019.

PAPANI, F. G.; SILVA, F. S. Um pouco da história da criptografia. **XXII Semana Acadêmica da Matemática,** Unioeste, p.1-6, 2021.

PRIETO, M. J. **Historia de la criptografia.** La Esfera de Los Libros. Madrid: Espanha, 2020 ISBN: 9788491647683

PRIMEIRO comando da capital–PCC. ***Insight Crime***, 2020. Disponível em: https://insightcrime.org/brazil-organized-crime-news/first-capital-command-pcc-profile/.

Acesso em 02 de Jul. de 2022.

QUEIROZ, Paulo. **Direito Penal**: parte geral. 4. ed. Rio de Janeiro: Lumen Juris, 2018.

RIBEIRO, J. A. **Liberdade e cumprimento de pena de presos no sistema carcerário Paranaense**. Curitiba (PR), 2019.

ROBERTO, Pascual, Daniel (2011). "Inteligencia criminal: una elección estratégica en clave de seguridad frente a la iniciativa de la delincuencia organizada", en: Fredy Rivera Vélez (editor). ***Inteligencia estratégica y prospectiva***. Quito: FLACSO / SE- NAIN / AECID: 215-238.

SANTOS, J. L**. A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica**. Dissertação de Mestrado (Mestrado em Matemática), 81 f, 2014.

SANTOS, L. P.; TAGLIAFERO, E. Aspectos dificultadores do bloqueio de telefones celulares em presídios brasileiros. **Revista Científica IntraCiência**, v. 1, n. 3, 2017.

SENNA, V. **Sistema Penitenciário Brasileiro**. Rio de Janeiro (RJ), 2020.

SILVA, Eduardo Araújo da. **Organizações criminosas**: aspectos penais e processuais da Lei nº 12.850/13. São Paulo: Atlas, 2014

SINGH, S. **O livro dos códigos**. 9 ed. Rio de Janeiro: Record, 2011. ISBN 8501055980.

SOUSA, Antônio Francisco. **A polícia no estado de direito**. São Paulo: Saraiva, 2009.

TEIXEIRA, S. W. D. **Estudo sobre a evolução da pena, dos sistemas prisionais e da realidade brasileira em execução penal.** Rio de Janeiro: Fundação Getúlio Vargas, 2018.

WALLACE, W. **A Evolução da Criptografia e Suas Técnicas ao Longo da História.** 29 f. Monografia (em Bacharelado em Sistemas de Informação). Instituto Federal Goiano, Campus Ceres, 2019.

WAZLAWICK, R. S. **História da Computação.** 1o edição. ed. Rio de Janeiro: Elsevier, 2016. ISBN 978853528546.

ZEHR, H. **Trocando as lentes**: um novo foco sobre o crime e a justiça. Tradução de Tônia Van Acker. São Paulo: Palas Athena, 2021.