

A Transversalidade da Prática do Profissional de História

Denise Pereira
(Organizadora)



 **Atena**
Editora

Ano 2019

Denise Pereira
(Organizadora)

A Transversalidade da Prática do Profissional de História

Atena Editora
2019

2019 by Atena Editora

Copyright © da Atena Editora

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira

Diagramação e Edição de Arte: Lorena Prestes

Revisão: Os autores

Conselho Editorial

- Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul
Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília
Profª Drª Cristina Gaio – Universidade de Lisboa
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa
Profª Drª Daiane Garabeli Trojan – Universidade Norte do Paraná
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista
Profª Drª Deusilene Souza Vieira Dall’Acqua – Universidade Federal de Rondônia
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná
Profª Drª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia
Profª Drª Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice
Profª Drª Juliane Sant’Ana Bento – Universidade Federal do Rio Grande do Sul
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul
Profª Drª Lina Maria Gonçalves – Universidade Federal do Tocantins
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte
Profª Drª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)

T772 A transversalidade da prática do profissional de história [recurso eletrônico] / Organizadora Denise Pereira. – Ponta Grossa (PR): Atena Editora, 2019. – (A transversalidade da Prática do Profissional de História; v. 1)

Formato: PDF

Requisitos de sistema: Adobe Acrobat Reader

Modo de acesso: World Wide Web

Inclui bibliografia

ISBN 978-85-7247-282-1

DOI 10.22533/at.ed.821192504

1. História – Estudo e ensino. 2. Prática de ensino. 3. Professores de história – Formação I. Pereira, Denise. II. Série.

CDD 907

Elaborado por Maurício Amormino Júnior – CRB6/2422

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores.

2019

Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

www.atenaeditora.com.br

APRESENTAÇÃO

A transversalidade da Prática do Profissional de História

Ao longo das últimas décadas, o ensino de História vem se consolidando enquanto campo de pesquisa, principalmente a partir da década de 1980, e as linhas de pesquisa, mormente, estão ligadas às metodologias de ensino, ao livro didático ou, ainda, às políticas públicas de inserção desses temas no currículo escolar. Neste modo, falar de transversalidade na prática do profissional de História, é observar a ligação aproximada da escola da realidade vivida pelos alunos, ou seja, trazer as disciplinas, os professores, os conteúdos escolares e aproximá-los do mundo do estudante. Dessa maneira, os alunos teriam uma aprendizagem significativa e seriam vistos com sujeitos históricos.

Os temas transversais são abordados recorrentemente a partir da proposta do trabalho interdisciplinar. O fato recorrente nessas abordagens interdisciplinares é que cada disciplina/campo se preocupa com seu recorte específico sobre o tema, o que acaba fragmentando-o ainda mais.

A aplicação dos temas transversais acontece a partir da renovação nos métodos, conceitos e didáticas no campo da pesquisa em História. Neste e-book temos a compreensão da realidade e a afetiva participação do indivíduo a partir de dados e noções relativos ao seu cotidiano, ao seu universo, fazem com que a campo do historiador a passe a ser considerada como um espaço de conhecimento e reconhecimento, onde por intermédio das diversas outras áreas de pesquisa se concretize como construtor de sua própria história.

Aqui diversos pesquisados do campo da História, trabalharam com a proposta de temas transversais em várias áreas baseadas em eixos temáticos, tais como: cultura, religião, educação, arte, cinema, gênero, entre muitos outros.

Boa leitura.
Denise Pereira

SUMÁRIO

CAPÍTULO 1	1
A DRAMATURGIA COMO FONTE PARA HISTÓRIA DA ILUMINAÇÃO CÊNICA, QUESTÕES DE ABORDAGEM PARA UMA PESQUISA EM ANDAMENTO	
Berilo Luigi Deiró Nosella	
DOI 10.22533/at.ed.8211925041	
CAPÍTULO 2	8
A EDUCAÇÃO PATRIMONIAL E ARTÍSTICA (EPA) COMO COMPONENTE CURRICULAR DAS ESCOLAS ESTADUAIS DA BAHIA: A EXPERIÊNCIA DO COLÉGIO DOUTOR JUCA SENTO-SÉ	
Angla Pereira dos Santos Rodrigues	
DOI 10.22533/at.ed.8211925042	
CAPÍTULO 3	14
A ESCOLARIZAÇÃO EM ITABORAÍ-RJ NO PERÍODO IMPERIAL (1840-1888)	
Regina Coeli Alcantara Silva	
DOI 10.22533/at.ed.8211925043	
CAPÍTULO 4	24
A FORMAÇÃO DE MÉDICOS NEGROS NAS ESCOLAS MÉDICAS BRASILEIRAS	
Helber Renato Feydit de Medeiros	
DOI 10.22533/at.ed.8211925045	
CAPÍTULO 5	31
A HISTÓRIA DO BAIRRO SÃO BENEDITO	
Marília Villanova Rodriguês	
DOI 10.22533/at.ed.8211925045	
CAPÍTULO 6	38
A LINHA DURA NACIONALISTA E A “NASSERIZAÇÃO FRUSTRADA” DO REGIME MILITAR BRASILEIRO	
Guillaume Azevedo Marques de Saes	
DOI 10.22533/at.ed.8211925046	
CAPÍTULO 7	46
A LITERATURA E O CORPO CONTRA O CASTRISMO: O RELATO AUTOBIOGRÁFICO DE REINALDO ARENAS (1943-1990)	
Bruna Alves Carvalho Mendes	
DOI 10.22533/at.ed.8211925047	
CAPÍTULO 8	54
A NAÇÃO NO BRASIL E NA COLÔMBIA: UMA ANÁLISE A PARTIR DO ESPORTE ¹	
Eduardo de Souza Gomes	
DOI 10.22533/at.ed.8211925048	
CAPÍTULO 9	65
A POLÍTICA INVADE O VERSO: REPRESENTAÇÕES DA REVOLUÇÃO DE 1848 NA POESIA DE BAUDELAIRE	
Marcos Antonio de Menezes	
DOI 10.22533/at.ed.8211925049	

CAPÍTULO 10	76
CONSERVADORISMO E PERSPECTIVA VARNHAGENIANA: ANÁLISE DE UM CONCEITO	
Ingrid Silva Lucas	
DOI 10.22533/at.ed.82119250410	
CAPÍTULO 11	85
DA IGREJA AO CAMPO SANTO: O NASCIMENTO DOS CEMITÉRIOS E O MONOPÓLIO DA MORTE NO BRASIL DO SÉCULO XIX	
Leonardo Oliveira Silva	
DOI 10.22533/at.ed.82119250411	
CAPÍTULO 12	99
DEMOCRACIA E AUTORITARISMO: Trajetória Política De Eduardo Gomes Em Contextos De Transições	
Flavia Salles Ferro	
DOI 10.22533/at.ed.82119250412	
CAPÍTULO 13	105
DO SUBVERSIVO AO TRAFICANTE: O PAPEL DA GUERRA ÀS DROGAS NA CONSTRUÇÃO DO “INIMIGO INTERNO” NO BRASIL	
Luiz Henrique Santos Brandão	
DOI 10.22533/at.ed.82119250413	
CAPÍTULO 14	120
ENSINO DE HISTÓRIA E O USO DO FILME: DIÁCONOS PELA DEFESA E JUSTIÇA E A CONSTRUÇÃO DO SABER DISCENTE	
Samara Letycia Moura Borges	
DOI 10.22533/at.ed.82119250414	
CAPÍTULO 15	127
ENTRE O DISFORME E O MONSTRO: O CORPO ESPETÁCULO	
Juçara de Souza Nassau	
DOI 10.22533/at.ed.82119250415	
CAPÍTULO 16	137
FUNÇÃO POLÍTICA DA MEMÓRIA E AFIRMAÇÃO INSTITUCIONAL	
Lindsay Borges	
DOI 10.22533/at.ed.82119250416	
CAPÍTULO 17	153
GÊNERO E DISCURSO NO CURDISTÃO SÍRIO: NOTAS DE PESQUISA	
Maria Raphaela Campello	
DOI 10.22533/at.ed.82119250417	
CAPÍTULO 18	166
GESTÃO DOS SENTIMENTOS POLÍTICOS: UMA ANÁLISE DO <i>FRONT NATIONAL</i> COM MARINE LE PEN	
Makchwell Coimbra Narcizo	
DOI 10.22533/at.ed.82119250418	

CAPÍTULO 19	179
HISTÓRIA E SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE A SEGUNDA GUERRA MUNDIAL E O DESENVOLVIMENTO DA CRIPTOGRAFIA A PARTIR DE UMA PERSPECTIVA INTEGRADA	
Rogério Chaves da Silva	
George Mendes Marra	
Delson Ferreira	
Geovane Reges de Jesus Campos	
Amivaldo Batista dos Santos	
DOI 10.22533/at.ed.82119250419	
CAPÍTULO 20	195
HISTÓRIA, IMPRENSA E PODER: FOLHA DE S. PAULO E O GLOBO COMO ATORES POLÍTICOS NAS ELEIÇÕES PRESIDENCIAIS DE 1994 E 1998	
Fabrício Ferreira de Medeiros	
DOI 10.22533/at.ed.82119250420	
CAPÍTULO 21	209
INFINITAS MARIAS Conhecendo as Marias desde 1950 PROPOSTA DE PRODUÇÃO DE MATERIAL DIDÁTICO	
Ronía Batista Vaz Otoni	
DOI 10.22533/at.ed.82119250421	
CAPÍTULO 22	217
JORNALISMO LITERÁRIO E PÓS-MEMÓRIA NA ÁFRICA COLONIAL PORTUGUESA DO SÉCULO XX: O CASO DOS LIVROS-REPORTAGEM SOBRE RETORNADOS	
Flávia Arruda Rodrigues	
DOI 10.22533/at.ed.82119250422	
SOBRE A ORGANIZADORA	226

HISTÓRIA E SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE A SEGUNDA GUERRA MUNDIAL E O DESENVOLVIMENTO DA CRIPTOGRAFIA A PARTIR DE UMA PERSPECTIVA INTEGRADA

Rogério Chaves da Silva

Professor do IF Goiano Campus Avançado
Hidrolândia-GO

George Mendes Marra

Mestre em História, Professor da Universidade
Estadual de Goiás/Trindade-GO

Delson Ferreira

Professor do IFGoiano Campus Avançado
Hidrolândia-GO

Geovane Reges de Jesus Campos

Professor do IFGoiano Campus Avançado
Hidrolândia-GO

Amivaldo Batista dos Santos

Professor do IFGoiano Campus Avançado
Hidrolândia-GO

RESUMO: Ancorados na perspectiva da formação integrada, elaboramos esse texto que foi concebido após a realização de um projeto integrador definido como “História, Criptografia e Segurança da Informação”. Por meio desse projeto, buscamos viabilizar a integração entre conhecimentos adquiridos em disciplinas da educação profissional, notadamente em “Segurança em Redes de Computadores” e “Redes de Computadores III”, com conhecimentos apreendidos em componentes curriculares da formação geral/propedêutica, sobretudo nos domínios da História, Filosofia e Sociologia. Nesse sentido,

procuramos propiciar, junto a estudantes do Curso Técnico em Manutenção e Suporte em Informática Integrado ao Ensino Médio do IF Goiano Campus Avançado Hidrolândia, um estudo focado na análise do desenvolvimento da criptografia no contexto da Segunda Guerra Mundial, destinando ênfase no modo como a invenção de Alan Turing, a chamada “bomba criptológica”, foi fundamental tanto para as estratégias vitoriosas do sistema de inteligência inglês naquele período de beligerância, como também para o desenvolvimento da computação moderna.

PALAVRAS-CHAVE: História Contemporânea; Segunda Guerra Mundial; Segurança da Informação; Criptografia; Formação Integrada.

ABSTRACT: Anchored in the perspective of integrated training, we elaborated this text that was conceived after the realization of an integrative project defined as “History, Cryptography and Information Security”. Through this project, we seek to enable the integration of knowledge acquired in professional education disciplines, notably in “Computer Network Security” and “Computer Networks III”, with knowledge learned in curricular components of general / propaedeutic training, especially in the domains of History, Philosophy and Sociology. In this sense, we seek to provide, together with students of the Technical Course in Maintenance

and Support in Integrated Computer Science at the High School of IF Goiano Advanced Campus Hidrolândia, a study focused on the analysis of the development of cryptography in the context of World War II, with emphasis on how the invention of Alan Turing, the so-called cryptological bomb, was central to both the victorious strategies of the English intelligence system in that period of belligerence and to the development of modern computing.

KEYWORDS: Contemporary History; Second World War; Information security; Cryptography; Integrated Training.

1 | A FORMAÇÃO INTEGRADA NO ÂMBITO DA EDUCAÇÃO PROFISSIONAL NO BRASIL

Esse texto é fruto de reflexões produzidas a partir de uma experiência pedagógica realizada por professores envolvidos em um projeto integrador executado no Instituto Federal Goiano, especificamente no Campus Avançado Hidrolândia, no ano de 2017, cujo título foi “História, Criptografia e Segurança da Informação”. Primeiramente, é preciso esclarecer que os Institutos Federais de Educação, Ciência e Tecnologia, como é o caso do IFGoiano, por pertencerem à Rede Federal de Educação Profissional e Tecnológica, têm como prioridade estabelecida pela Lei Federal nº 11.892/2008 a oferta de cursos de educação profissional de nível médio na modalidade integrada. A partir de nossa atuação como professores nesses cursos chamados, comumente, de “Ensino Médio Integrado” que concebemos o projeto integrador intitulado “História, Criptografia e Segurança da Informação”, cuja experiência propiciou essa reflexão didático-pedagógica que aqui materializamos em texto. O projeto em questão foi executado na 3ª série do Curso Técnico em Manutenção e Suporte em Informática Integrado ao Ensino Médio do Campus Avançado Hidrolândia, pertencente ao Instituto Federal Goiano.

Os cursos técnicos de “Ensino Médio Integrado” foram implementados na Rede Federal a partir do Decreto nº 5.154/2004 que, posteriormente, foi regulamentado pela Lei Federal nº 11.741/2008. Ambos os dispositivos jurídicos estabeleceram novas diretrizes para a educação profissional no Brasil, principalmente no tocante à oferta de cursos da educação profissional técnica de nível médio. Os artigos 36-B e 36-C dessa lei (que ainda está em vigor) definiram as características dessa modalidade de ensino:

Art. 36-B. A educação profissional *técnica* de nível *médio* será *desenvolvida* nas seguintes formas:

I – articulada com o ensino *médio*;

II – subsequente, em cursos destinados a quem já tenha concluído o ensino *médio*;
(...)

Art. 36-C. A educação profissional *técnica* de nível *médio* articulada, prevista no inciso I do caput do art. 36-B desta Lei, será desenvolvida de forma:

I - integrada, oferecida somente a quem já tenha concluído o ensino fundamental, sendo o curso planejado de modo a conduzir o aluno à habilitação profissional *técnica* de nível *médio*, na mesma instituição de ensino, efetuando-se matrícula *única* para cada aluno

(LEI FEDERAL Nº 11.741 DE 16 DE JULHO DE 2008)

Para as reflexões inscritas a esse texto, importa-nos salientar o inciso I do Art. 36-C, que norteia a articulação, de forma **integrada**, entre a educação profissional técnica de nível médio e o ensino médio, de modo que se atenda a formação geral do educando. O núcleo dessa proposta, subsumida aos “Cursos de Ensino Médio Integrado”, reside na tentativa de superar o modelo de ensino, muito comum nas escolas de educação profissional das últimas décadas do século XX, em que a preparação para o trabalho estava voltada apenas para o seu aspecto operacional. Ao se dar relevo à formação integrada, articulando o ensino regular com o técnico, busca-se integrar, efetivamente, a educação geral com a educação profissional, pois mesmo que o foco educacional esteja mirado à preparação do educando para o mundo do trabalho, sua formação humanística torna-se essencial para a construção de indivíduos questionadores, críticos, conscientes de seu papel na sociedade, em suma, cidadãos na acepção da palavra. De acordo com a professora Maria Ciavatta (2005), a formação integrada tem como características:

O que é integrar? É tornar íntegro, tornar inteiro, o que? No caso da formação integrada ou do ensino médio integrado ao ensino técnico, queremos que a educação geral se torne parte inseparável da educação profissional em todos os campos onde se dá a preparação para o trabalho: seja nos processos produtivos, seja nos processos educativos como a formação inicial, como o ensino técnico, tecnológico ou superior. Significa que buscamos enfocar o trabalho como princípio educativo, no sentido de superar a dicotomia trabalho manual / trabalho intelectual, de incorporar a dimensão intelectual ao trabalho produtivo, de formar trabalhadores capazes de atuar como dirigentes e cidadãos (CIAVATTA, 2005, p. 02)

Historicamente, a discussão acerca da educação integrada tem como preocupação central a superação da dicotomia trabalho manual versus trabalho intelectual. No Brasil, a sedimentação do dualismo entre trabalho manual e o intelectual tem suas raízes históricas fincadas em uma sociedade de herança cultural ibérica e escravocrata, em que o trabalho manual era tratado como “inferior”, “subalterno”, papel do escravo. Do ponto de vista institucional, somente no século XX é que a educação das camadas sociais menos privilegiadas passou a ser uma preocupação do Estado, quando o problema do analfabetismo ganhou a atenção governamental. Dentro desse contexto, configurou-se uma transparente dicotomia entre a educação voltada para as elites e o modelo destinado às classes desvalidas: a formação intelectual era monopolizada pelas elites dirigentes, enquanto a preparação para o mundo do trabalho era dirigida aos desamparados.

Tal concepção implicava na distinção entre os que concebiam e controlavam o processo de trabalho e aqueles que o executavam. O ensino profissional era destinado àqueles que deviam executar, ao passo que o ensino científico-intelectual era voltado àqueles que concebiam e controlavam o processo. A perspectiva da formação integrada, preconizada pelo Decreto nº 5.154/2004, veio se contrapor a essa ideia, postulando que o processo de trabalho desenvolva, em uma unidade indissolúvel, os aspectos manuais e intelectuais. Um pressuposto dessa concepção é que não existe trabalho manual puro e nem trabalho intelectual puro. Todo trabalho humano envolve a concomitância do exercício dos membros, das mãos, e do exercício mental, intelectual. Portanto, a formação integrada entre o ensino geral e a educação profissional exige a superação das dualidades entre cultura geral e cultura técnica, entre instrução profissional e instrução geral, para assim, incorporar a dimensão intelectual ao trabalho produtivo, de modo a preparar trabalhadores capazes de atuar como dirigentes e cidadãos.

Em suma, a educação profissional, articulada à escolarização básica, constitui um processo formativo integral que intenta compreender a problemática social em que os jovens estão inseridos como sujeitos de direitos e de ações na sociedade. Ao mesmo tempo, procura contribuir para a sua inserção na vida adulta e no mundo do trabalho como cidadãos e sujeitos autônomos. De acordo com esse postulado educacional, a apropriação de saberes e conhecimentos, referentes à ciência e à cultura, possibilita ao futuro trabalhador a percepção da complexidade do mundo em que vive e, de igual forma, viabiliza sua preparação para as exigências da vida profissional.

Inspirados nessa perspectiva da formação integrada, concebemos o projeto integrador “História, Criptografia e Segurança da Informação”. O objetivo central era o de possibilitar a integração entre conhecimentos adquiridos nas disciplinas da educação profissional (como, por exemplo, “Segurança em Redes de Computadores” e “Redes de Computadores III”), constituintes da matriz curricular do curso técnico em manutenção e suporte em informática, com conhecimentos apreendidos em componentes curriculares da formação geral/propedêutica (como História, Filosofia e Sociologia), também constantes nessa matriz curricular.

O interesse em adentrar nesse tema se assentou no fato de que a maioria das pessoas usa configurações básicas de criptografia em equipamentos eletrônicos que fazem parte do cotidiano, como telefones celulares e computadores pessoais. No entanto, poucas pessoas têm conhecimento de que, durante a Segunda Guerra Mundial, as estratégias de comunicação e de codificação de mensagens entre os países beligerantes, por meio da criptografia, foram fundamentais não só para a constituição da computação moderna, como também para a preservação de informações sigilosas como as que trafegam, atualmente, na rede mundial de computadores (Internet). Partindo da reflexão sobre essas questões que permeiam a tecnologia e a informação na contemporaneidade, decidimos que a relação entre história e segurança da

informação seria o eixo norteador desse estudo voltado para a compreensão e análise do desenvolvimento da criptografia, sobretudo no contexto da Segunda Guerra Mundial, e suas reverberações na moderna computação e no tráfego sigiloso das comunicações oficiais entre os países e também nas informações privadas que transitam pela Internet.

2 | BREVES ANOTAÇÕES HISTÓRICAS SOBRE A CRIPTOGRAFIA

A criptografia é uma das principais áreas da criptologia. Basicamente, são três as áreas subsumidas à criptologia: a esteganografia, a criptografia e a criptoanálise. A criptografia consiste na ocultação de informações e na quebra do sigilo dos códigos de ocultação (criptoanálise). As mensagens podem ser ocultadas de formas distintas: ocultando a existência da mensagem (esteganografia) ou tornando seu conteúdo não inteligível (criptografia). Na criptografia, destacam-se os códigos e as cifras. As cifras podem ser de substituição ou de transposição. Observe a figura a seguir:

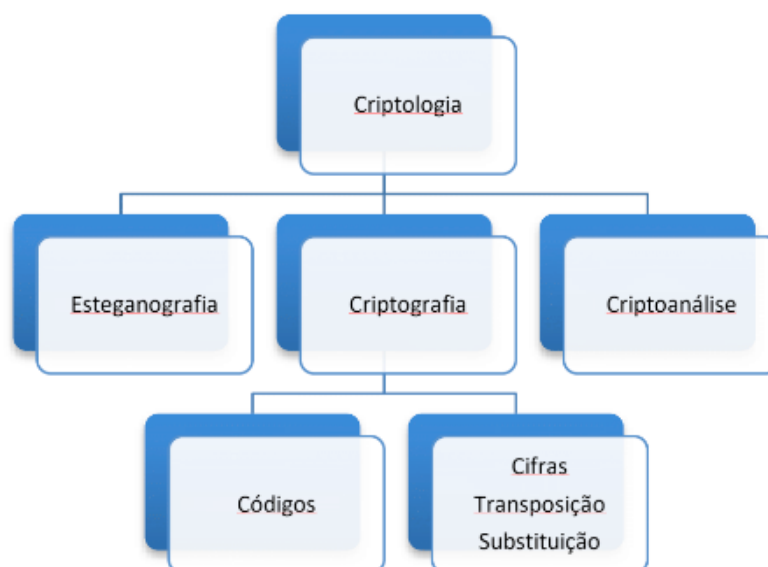


Figura 1 - Áreas da Criptologia

Fonte: MARRA, 2017, p. 87

A criptografia é comumente conhecida como a arte de cifrar/codificar uma mensagem como mecanismo de segurança. Etimologicamente, o termo é grego, no qual *Krytos* significa aquilo que é descrito de forma oculta, escondida, enquanto *Graphos* significa o ato de escrever (TKOTZ, 2005, p. 16). Ao afirmar que o texto está criptografado, isso quer dizer que as informações foram tornadas inteligíveis por meio de substituições de caracteres que compõem a mensagem de uma maneira que somente aqueles que possuem a chave podem tornar aquilo compreensível. A decodificação refere-se ao ato, praticado por um usuário legítimo do código, na busca por compreender a mensagem codificada. Já a decifração está ligada ao ato de ler a

mensagem codificada sem ser um usuário legítimo do código. Portanto, a criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la.

Na criptografia, é necessário o uso dos chamados números aleatórios criptograficamente fortes. Quando este tipo de número é gerado, o inimigo não pode nem desconfiar qual o número escolhido. Se o inimigo reproduzir o processo de geração do número e/ou limitar a faixa de valores, então, esse número não é adequado para a criptografia.

Tanto a criptografia quanto a criptoanálise, até recentemente, eram consideradas uma arte. A criptologia vem ganhando um destaque maior há aproximadamente vinte anos, quando foi reconhecida como ciência. A *International Association for Cryptologic Research* (IACR ou Associação Internacional para a Pesquisa Criptológica) é a organização científica internacional que coordena a pesquisa nesta área. A criptologia como ciência é recente, mas sua história remonta os primórdios da humanidade (TKOTZ, 2005, p. 16).

A criptografia começou a ser praticada já na Antiguidade. Os hebreus, por exemplo, nas imediações de 600 a.C., desenvolveram cifras de substituição monoalfabéticas (nas quais um símbolo do alfabeto é substituído por outro símbolo no alfabeto cifrado), como a cifra *Atbash*, que consiste na substituição da primeira letra do alfabeto pela última, da segunda pela penúltima, e assim por diante. Com o início das pesquisas sobre criptoanálise por volta de 800 d.C., o matemático árabe Ibrahim Al-Kadi inventou a técnica de análise de frequência para quebrar esse tipo de cifra. Ele também expôs métodos de cifragem como, por exemplo, a criptoanálise de certas cifragens e a análise estatística de letras e combinações de letras em árabe.

Antes da Primeira Guerra Mundial, no século XX, poucas inovações haviam sido desenvolvidas no campo de criptografia. Até que Alexander's Weekly escreveu um ensaio sobre métodos de criptografia, que se tornou útil como uma introdução para os criptoanalistas britânicos na quebra dos códigos e cifras alemães durante a chamada "Guerra Total" (1ª Guerra). Além de ser um importante instrumento de quebra de códigos navais alemães, que chegaram a decidir o destino de batalhas, a contribuição mais importante do uso de seus conceitos, foi decodificar o telegrama de Zimmermann, enviado ao embaixador alemão no México, Heinrich Von Eckardt, instruindo-o a se aproximar do governo mexicano e propor uma aliança militar contra os Estados Unidos, em troca ele prometia ao México terras norte-americanas, caso o país aceitasse o acordo. O telegrama foi interceptado pela Inglaterra e enviado ao governo norte americano, o que apressou a entrada dos Estados Unidos na Primeira Guerra Mundial.

Durante a Segunda Guerra Mundial, os alemães usaram uma máquina eletromecânica para criptografar e descriptografar, denominada de Enigma. Durante o conflito, o governo britânico reuniu um grupo de criptógrafos (alguns matemáticos e mestres em xadrez) em *Bletchley Park* para decifram as mensagens enviadas pela

máquina Enigma. Esses criptoanalistas, capitaneados pelo matemático Alan Turing, considerado o pai da computação moderna, conseguiram quebrar as cifras da Enigma e decifrar mensagens secretas dos nazistas. Os militares alemães implantaram máquinas usando *one-time pad* (cifra de chave única), um algoritmo de criptografia no qual o texto é combinado com uma chave aleatória; enquanto isso, os ingleses criaram o primeiro computador digital programável, o *Colossus*, para ajudar com sua criptoanálise. O *Colossus* foi construído para fazer cálculos “booleanos”: um métodos de trabalhar com processos lógicos usando símbolos; em outras palavras, expressar ideias como “verdadeiro, falso”, ou “e, ou”, puramente em termos binários de zeros e uns, ou sinais ligado/desligado (*on/off*). A inspiração muito se deve a Alan Turing, o matemático de Cambridge que “inventou” a ideia do computador como uma “experiência de pensamento”, para enfrentar problemas matemáticos por meios mecânicos.

Turing desenvolveu um sistema chamado “*bombe*”, para traduzir os textos secretos dos alemães, gerados por máquinas de criptografia chamadas de “Enigma”. A *bombe* traduzia comunicações codificadas pela Enigma, transformando-as em uma mensagem verdadeira e compreensível. Porém, seu grande feito foi a criação da Máquina de Turing. Uma invenção automática capaz de manipular símbolos em uma fita de acordo com uma série de regras para guardar informação, exatamente como os computadores fazem hoje em dia. Turing desenvolveu conceitos de algoritmo – uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa – e computação. Também “escreveu” o primeiro programa de xadrez para computador. Mesmo com todas essas invenções, ainda sobrava tempo para se dedicar à química, à física e à biologia.

Alan Turing desenvolveu ainda o Teste de Turing, criado com o objetivo de verificar se o computador é capaz de imitar e pensar como o cérebro humano, ou seja, uma espécie de inteligência artificial com possibilidade de enganar qualquer um. O teste consistia em pedir a uma pessoa que mandasse uma série de perguntas para o computador e, depois de analisar as respostas dadas por ele, tentar diferenciar se a resposta dada pelo sistema foi elaborada pelo ser humano ou pela máquina.

Após a Segunda Guerra Mundial, na chamada “Guerra Fria” protagonizada por Estados Unidos e União Soviética, foram criados e utilizados diversos métodos para esconder mensagens com estratégias e operações. Desses esforços, surgiram outros tipos de criptografia, tais como: por chave simétrica, na qual existe uma chave com um segredo e essa chave é compartilhada pelos interlocutores; por chave assimétrica, na qual existem duas chaves, uma pública e uma privada. A chave privada é usada para cifrar a mensagem, com isso garante-se que apenas o dono da chave poderia tê-la editado; por *hash* e até a chamada criptografia quântica, que se encontra, hoje, em desenvolvimento.

Atualmente, a criptografia é comumente usada na Internet, principalmente na proteção de transações financeiras, em segurança e acesso das comunicações. As transações bancárias, as conexões em redes sem fio, o uso dos pacotes de TV

a cabo, ou também na utilização de cartões de crédito, são operações que fazem parte de nossa vida cotidiana. Nessas operações, as informações trafegadas estão, intrinsecavelmente, permeadas por segredos e, portanto, ligadas à segurança da informação. As conversas por telefone celular, ou aquelas mediadas via aplicativos, como *Whatsapp* por exemplo, se não houvesse proteção, poderiam ser ouvidas ou acessadas por qualquer pessoa que acessasse o sinal naquela área ou invadisse o aplicativo. Não obstante, essa proteção oferecida nem sempre garante total proteção, até porque são sistemas vulneráveis. É só observarmos a quantidade de *hackers* que invadem contas bancárias e fazem transações financeiras que desafiam os sistemas de segurança dos bancos.

Refletindo sobre o desenvolvimento da criptografia na história da humanidade, bem como em sua atualidade nos processos de comunicação, entendemos que seria importante confeccionar um projeto que destinasse relevo ao estudo da criptografia, pois seu desenvolvimento no século XX, notadamente durante e após a Segunda Guerra Mundial, guarda estreita relação com a própria origem da computação moderna. A importância desse tema ganha ainda mais vigor ao considerarmos que a criptografia é essencial para a troca de informações através da Internet, como mencionamos anteriormente. No entanto, mesmo com tanta segurança, a criptografia jamais será capaz de garantir absoluta integridade do conteúdo. Sempre vão existir pessoas capazes de desenvolver técnicas para quebrar estas chaves, por este motivo é que novas técnicas são criadas a cada dia e as existentes aperfeiçoadas. Todos utilizam a criptografia, a diferença é que na computação ela é aplicada sem que a maioria das pessoas saiba disso.

3 I “O JOGO DA IMITAÇÃO”: PONTO DE PARTIDA PARA REFLEXÃO SOBRE O TEMA PROPOSTO

É incontestável que vivenciamos, em escala global, não só a “Era da Informação”, na qual as notícias e as informações circulam em uma velocidade exorbitante, como também a “Era das Imagens”, em que, por meio de um *smartphone* ou de outros recursos audiovisuais, as imagens são produzidas e reproduzidas de forma extraordinária mundo afora. Nesse contexto, não há como negar que, na contemporaneidade, os jovens vivem essas experiências informacionais e imagéticas com uma intensidade nunca vista na história da humanidade. Destarte, entendemos que as novas linguagens informacionais e culturais, como a internet e os filmes, podem se converter em aliadas do professor nos processos de ensino e de aprendizagem, principalmente, no sentido de despertar o interesse do aluno em relação a temas e conteúdos abordados em sala de aula.

Acreditamos que as narrativas audiovisuais também são formas discursivas capazes de representar o passado. Logicamente, é importante considerar as

peculiaridades dos discursos audiovisuais, sobretudo no que concerne a complexa relação entre o que é fato histórico, baseado em fontes históricas, e aquilo que é produto da ficção. Buscamos, assim, trabalhar com a produção cinematográfica como meio de discussão de um tema histórico, notadamente a Segunda Guerra Mundial, com foco no desenvolvimento da criptografia. Não obstante, é preciso realçar que a exibição do filme esteve permeada por uma perspectiva crítica, na qual tivemos a preocupação em discutir que a película exibida não se tratava de verdade absoluta, e sim de uma narrativa audiovisual que nos possibilita acessar determinadas especificidades relativas ao tempo, espaço e sobre os sujeitos históricos envolvidos na época em pauta. Para além do mero interesse em “assistir a um filme”, pretendíamos extrair da narrativa fílmica questões profícuas à reflexão sobre a temática eleita. Almejamos, por conseguinte, problematizar aspectos presentes nas entrelinhas dessa narrativa, analisando os significados latentes e os explícitos, sobretudo, aqueles relacionados ao desenvolvimento de estratégias secretas de informações em meio a um período de beligerância.

Ancorados nessa premissa, decidimos exibir o filme “O Jogo da Imitação” como ponto de partida para a reflexão sobre a importância da criptografia no contexto da Segunda Guerra Mundial. Esse filme foi escolhido pois traz em seu enredo a trajetória Alan Turing, criptologista inglês que, no contexto da Segunda Guerra Mundial, foi fundamental para a decifração dos códigos alemães feitos por intermédio das máquinas Enigma. O filme “Jogo da Imitação” foi baseado no livro *“Alan Turing: The Enigma”*, de Andrew Hodges. Por meio da narrativa biográfica sobre Turing, é possível compreender o gigantesco esforço feito pelos países aliados para decifrar as mensagens secretas da Alemanha nazista. Turing foi um dos grandes cientistas que ajudou a desvendar os segredos do sistema Enigma, o que auxiliou na vitória dos aliados, capitaneados pela Inglaterra, França e Estados Unidos.

O filme “O Jogo da Imitação”, cujo título original é *“The Imitation Game”*, foi lançado em 2014. Produzido por profissionais do Reino Unido e Estados Unidos, o longa foi dirigido pelo norueguês Morten Tyldum, cuja produção contou com Nora Grossman, Ido Ostrowsky e Teddy Schwarzman. O roteiro foi feito por Graham Moore. O ator Benedict Cumberbatch interpretou Alan Turing e, inclusive, foi indicado ao Oscar de melhor ator por essa brilhante atuação. Óscar Faura foi o responsável pela cinematografia e a edição assinada por William Goldenberg.

O enredo do filme retrata parte da trajetória do cientista inglês Alan Turing (1912-1954), desde a infância, nos anos 1920, quando estudava em um colégio interno, até sua atuação em um grupo de criptologistas instalados em um lugar secreto na Inglaterra chamado de *Bletchley Park*, durante a Segunda Guerra Mundial. Também conhecido como *Station X*, *Bletchley Park* era uma espécie de esconderijo onde esse grupo de criptologistas decodificava as mensagens criptografadas pelas máquinas Enigma alemãs. O filme demonstra como o domínio da informação pelos ingleses foi crucial durante esse conflito mundial que durou de 1939 a 1945. Os alemães, durante

a guerra, detinham a rede de comunicação mais segura do mundo.

Com o início do conflito, o governo da Grã-Bretanha acelerou o recrutamento de matemáticos, linguistas e criptoanalistas com o objetivo de decifrar os códigos secretos da máquina Enigma alemã. Foi nesse contexto que o comandante Alastair Denniston conheceu Alan Turing. Depois de recusar uma oferta para trabalhar como assistente de John Von Neumann em Princeton, Turing retornou à Inglaterra, onde foi convocado para um curso de criptografia e encriptação conduzido pela *Government Code and Cipher School*, em Londres. De algum modo, o interesse de Turing por códigos e quebra de códigos, sem mencionar seu talento para a matemática, tinha chegado aos ouvidos do comandante Alastair Denniston, o diretor da escola (LEAVITT, 2011, p. 151)

De posse de um modelo de uma máquina Enigma que foi capturada pelos poloneses em Berlim, os cientistas ingleses, dentre eles Turing, começaram o trabalho para decifrar algumas palavras por meio de análise de frequência da distribuição das cartas, mas o volume de informações diárias tornava a tarefa quase impossível. As mensagens alemãs sempre começavam com cinco letras aleatórias, entretanto, alguns operadores alemães colocavam nomes próprios no início das mensagens. Com isso, tornavam essas mensagens decifráveis pela posição das letras e era possível gerar a chave criptográfica do dia. Sob o nome código “ultra”, um dos maiores serviços de inteligência da história, os ingleses puderam decifrar diversas mensagens criptografadas pela máquina Enigma alemã. Outro desafio seria o de escolher, pontualmente, quais ataques alemães seriam interceptados, para que eles não desconfiassem que o código da máquina Enigma tinha sido decifrado. É importante ressaltar, contudo, que o processo de decifragem da Enigma levou quase dois anos. Nesse período, os alemães já haviam conquistado, praticamente, quase toda a Europa.

Segundo Masson (2015), *Bletchley Park* contribuiu na Batalha do Atlântico (1939-1945) com informações que aumentaram a segurança dos comboios e melhorou o serviço de localização de submarinos alemães. De 1940 a 1943, os ingleses souberam explorar a falha da tática de “alcateias” com a utilização intensiva das comunicações pelo rádio. O código secreto da máquina Enigma naval foi decifrado duas vezes. De início, durante o segundo semestre de 1941. Os alemães modificaram a máquina Enigma e as cifras do codinome “*Triton*”. A segunda decifração ocorreu em novembro de 1942. Em março de 1943, os criptoanalistas de *Bletchley Park* não conseguiram decifrar as mensagens da marinha alemã, mas a captura de máquinas Enigma e seus livros de cifras a bordo de dois submarinos alemães avariados contribuíram para retomar o serviço de decifragem das mensagens.

As decifragens de *Bletchley Park* foram da maior importância. Por exemplo, quando a Alemanha invadiu a Dinamarca e Noruega em abril de 1940, *Bletchley* forneceu uma imagem detalhada das operações alemãs. De modo semelhante, durante a Batalha da Inglaterra (1940), os criptoanalistas foram capazes de dar alerta prévio dos ataques dos bombardeios, incluindo horas e os locais. Eles também podiam

fornecer dados, continuamente, atualizados sobre o estado da *Luftwaffe*, tais como número de aviões que tinham sido perdidos e a velocidade com que estavam sendo substituídos. Os criptoanalistas ingleses enviavam todas essas informações para a sede do MI6, que as repassava para o Ministério da Guerra, para o Ministério da Aeronáutica e o Almirantado (SINGH, 2014, p. 183-184)

Segundo Zochio (2016), *bombe* era o nome de uma máquina eletromecânica desenvolvida durante a Segunda Guerra Mundial por Alan Turing e Gordon Welchman quando trabalhavam em *Bletchley Park*. A *bombe* inglesa era parcialmente baseada na *bomb* polonesa. Turing usou uma abordagem diferente da máquina polonesa. Sua estratégia era se basear no ataque do texto conhecido, onde se conhece ou supõe-se que um texto chamado crib (berço), aparece em alguns lugares no texto. Gordon Welchman criou a placa diagonal que reduziu consideravelmente o número de combinações para decifração das mensagens.

Quando a *bombe* ou “bomba criptológica” de *Bletchley Park* ficou pronta, Turing e sua equipe ainda não sabiam como iam decifrar os códigos secretos da máquina Enigma. Devido ao grande número de combinações que a máquina Enigma oferecia, tinham que realizar os testes até a meia-noite. Exatamente à meia-noite, os alemães mudavam as configurações da Enigma e os criptoanalistas ingleses tinham que começar os testes a partir do zero. A primeira mensagem enviada pelos alemães era sobre o tempo, exatamente, às 06h da manhã.

A questão da homossexualidade de Alan Turing também foi tratada na narrativa do filme. Turing havia descoberto que John Cairncross era o espião soviético infiltrado na equipe de *Bletchley Park*. Em contrapartida, Cairncross tinha conhecimento que Alan Turing era homossexual. Cairncross ameaçou contar para o Comandante Deninnston que Turing era homossexual caso ele contasse sobre a espionagem soviética. É fundamental mencionar que a homossexualidade era proibida na Grã-Bretanha no contexto dos anos 1930 e 1940. Após o fim do conflito, Turing, em 1952, foi condenado por “atos homossexuais”. Para não ser preso, aceitou fazer o “tratamento” de castração química. Cansado de suportar a dor do tratamento hormonal e o constrangimento por mais tempo, em uma manhã de 1954, Turing preparou uma mistura de cianeto em seu laboratório em casa, injetou em uma maçã e, em seguida, deu uma mordida, morrendo em poucos minutos.

4 | ESTRUTURANDO O PROJETO: SEGUNDA GUERRA E CRIPTOGRAFIA

Como já mencionado alhures, o projeto integrador consiste em uma ferramenta metodológica que tem por característica básica a integração entre componentes curriculares da formação geral/propedêutica, aquelas consideradas da base nacional comum (como Língua Portuguesa, História, Geografia, Matemática, dentre outros) e componentes curriculares referentes à educação profissional (como Segurança em

Redes de Computadores, Tópicos Especiais em Computação, Redes de Computadores III, dentre outros). No caso específico do projeto em questão, o objetivo central foi o de analisar o uso da criptografia no contexto da Segunda Guerra Mundial e o modo como a invenção de Alan Turing, a “bomba criptológica”, foi fundamental para a computação moderna, sobretudo no que tange à segurança da informação em banco de dados e em redes de computadores (conteúdos estudados na 3ª série do Curso Técnico em Manutenção e Suporte em Informática Integrado ao Ensino Médio).

Pensando nos conteúdos que seriam ministrados, definimos os objetivos específicos subsumidos a essa proposta de formação integrada: analisar a importância da segurança da informação nas relações internacionais, sobretudo, no contexto da Segunda Guerra Mundial; compreender a criptografia como um dos principais instrumentos de comunicação secreta realizada entre as forças militares nazistas; contextualizar e compreender o contexto filosófico e sociológico do filme “O Jogo da Imitação” (*The Imitation Game*); analisar a criptografia utilizada em segurança da informação dos sistemas contemporâneos com a criptografia anacrônica, sem uso de tecnologia digital; apresentar as diversas formas de criptografia seguindo uma ordem cronológica da evolução dessa tecnologia; demonstrar os algoritmos: “Hash md5”, “Sha01” e “Esteganografia”, que criptografam informação por meio de linguagem de programação java e, finalmente, discutir a influência da criptografia na segurança dos bancos de dados e nas redes de computadores.

Ancorados nesses conteúdos e objetivos, estruturamos o projeto integrador em quatro etapas principais. Na primeira etapa, exibimos o filme “O Jogo da Imitação”, que narra a vida de Alan Turing, célebre matemático britânico, criador da chamada “bomba criptológica”, que decifrou a máquina Enigma, responsável pelas mensagens criptografadas pelo exército nazista durante a Segunda Guerra Mundial. O filme foi o ponto inicial de reflexão sobre o tema central do projeto. Na segunda etapa, realizamos docências compartilhadas, que consiste em aulas ministradas, ao mesmo tempo, por mais de um(a) docente como forma de enriquecer o processo educacional na medida em que são ministrados os conteúdos inerentes a cada componente curricular envolvido no projeto e, simultaneamente, os professores que estão em sala de aula medeiam discussões sobre os temas candentes do projeto. Foram realizados cinco encontros de docências compartilhadas, cada um com uma duração específica. Nesses encontros, os professores das disciplinas de Segurança em Redes de Computadores, Tópicos Especiais, Redes de Computadores III abordaram conceitos relativos à criptografia, esteganografia e suas aplicações na segurança de redes e de banco de dados. Além disso, analisaram o quanto a “bomba criptológica” de Turing foi fundamental para o desenvolvimento da computação no mundo contemporâneo. Em outros encontros, os professores de História, Sociologia, Filosofia e de Segurança em Redes de Computadores III abordaram o contexto histórico dos anos 1930 e 1940, quando a criptografia foi utilizada em larga escala pelos nazistas como forma de transmitir mensagens ultrassecretas, principalmente em momentos de beligerância.

Foi dada ênfase às principais ofensivas feitas tanto por Aliados quanto pelo Eixo Roma-Tóquio-Berlim, analisando as estratégias militares e políticas envolvidas nas principais operações e batalhas ocorridas durante a Segunda Guerra, tais como a ofensiva nazista sobre a Polônia e a França, a retirada de *Dunkirk*, a Batalha do Atlântico, a Batalha da Inglaterra, a Operação Barbarossa, o ataque japonês a *Pearl Harbour*, a Batalha de Stalingrado, a Batalha de *Midway*, a invasão da Normandia (Dia “D”) e tomada da Alemanha pelos Aliados. Abordou-se, também, o tema acerca do ocaso do projeto iluminista de modernidade, baseado em um otimismo em relação às potencialidades da razão, a crítica da razão instrumental feita pelos pensadores da Teoria Crítica/Escola de Frankfurt, na medida em que o conhecimento científico, o progresso, foi instrumentalizado em favor da “indústria da morte”, evidenciado nas duas grandes guerras mundiais. Também discutiu-se, historicamente, a questão da homossexualidade no contexto dos anos 1930 a 1950, quando Turing foi acusado de crime por “atos homossexuais”, e como o tema é tratado na contemporaneidade, sobretudo após a revolução cultural ocorrida a partir dos anos 1960 no mundo ocidental.

Na terceira etapa, a partir das discussões feitas entre professores e alunos(as), elegemos cinco temas que seriam objeto de pesquisa bibliográfica para que os(as) estudantes, posteriormente, realizassem seminários, os quais se constituiriam na culminância do projeto. Os temas escolhidos foram: história da criptografia, engenharia social - conceitos filosóficos e sociológicos, criptografia sem tecnologia, criptografia com tecnologia e a criação de um modelo criptográfico. Tendo em vista as temáticas selecionadas, cada grupo realizou sua pesquisa bibliográfica para que pudesse elaborar as respectivas apresentações dos seminários. Cada grupo foi orientado por um docente que tinha mais afinidade com o tema escolhido.

A quarta (e última) etapa consistiu na realização dos seminários que foram elaborados pelos próprios alunos a partir da pesquisa bibliográfica feita e da orientação dos professores envolvidos no projeto. Cada grupo, composto por quatro alunos(as), expôs sua temática por um período de até uma hora, sendo que, após cada apresentação, foi promovida uma discussão ampla sobre o tema apresentado, sendo que os professores finalizavam comentando a exposição feita. Ao final das apresentações, indagamos aos alunos sobre a percepção que tiveram sobre o projeto como um todo e acerca da prática da formação integrada.

5 | À GUIA DE CONCLUSÃO... AVALIANDO QUESTÕES HISTÓRICAS E EDUCACIONAIS

Avaliando do ponto de vista histórico, foi importante os(as) alunos(as) perceberem como são importantes as estratégias de comunicações secretas entre os países em contextos de beligerância, o que não foi diferente no caso da Segunda Guerra Mundial, evento histórico que circundava o estudo proposto. Mostramos que os alemães tinham

a rede comunicações mais segura do mundo no início do conflito e que o domínio dessas informações pelos ingleses, por meio da ação de criptoanalistas, foi crucial para as estratégias militares dos Aliados. No campo de batalha, os alemães demonstravam seu poderio bélico através da chamada *blitzkrieg* (“guerra relâmpago”), que acabava deixando o inimigo confuso a partir da combinação de veículos blindados, tanques de guerra, aviação e divisões secundárias atuando em sincronismo. Em alguns casos, a *blitzkrieg* contava com a participação ainda da marinha de guerra alemã que, juntamente com as comunicações (via rádio) criptografadas pela máquina Enigma, tornaram as Forças Armadas alemães quase imbatíveis no período de 1939 a 1941. Com as conquistas alemãs sobre a França, Bélgica e Holanda, a Grã-Bretanha ficou, praticamente, isolada nos dois anos iniciais do conflito, dependendo dos comboios de suprimentos vindos de suas colônias e, principalmente, dos Estados Unidos. Nesse contexto, era fundamental para os Aliados, em especial para a Grã-Bretanha, ter acesso às comunicações que eram feitas pelas Forças Armadas alemãs. Daí a importância de se compreender como o confronto entre os sistemas de inteligência de alguns países envolvidos no conflito foi essencial para a vitória de um bloco ou de outro. Nesse sentido, foi de fundamental importância estudar a atuação dos criptoanalistas de *Bletchley Park*, especialmente Alan Turing, um dos grandes responsáveis pela decifração da máquina Enigma dos alemães.

Esse trabalho de decifrar o código Enigma contou com o esforço de muitos criptoanalistas e, de algum modo, contribuiu para a fabricação do primeiro protótipo de um grande computador chamado *Colossus*. Interessante é que a Inglaterra manteve essa parafernália tecnológica oculta até 1975 e o algoritmo utilizado permanece secreto (MATO, 2016, p. 180). Atualmente, *Bletchley Park*, ao norte de Londres, funciona como museu onde é possível ver o *Colossus*, uma máquina de 5 metros de comprimento por 2 metros de altura. A construção do *Colossus* foi baseada em um sistema binário inspirado nos princípios de Alan Turing. A máquina em exibição no museu é a reconstrução do modelo original que foi mantido oculto até a década de 1970. Em *Bletchley Park* também se pode ver o último modelo da máquina de criptografia Enigma.

Foi importante esclarecer, também, que, em 2013, a Rainha Elizabeth II concedeu a Turing o perdão póstumo pelos seus préstimos e conquistas sem precedentes. Alguns historiadores chegaram a afirmar que, com a decifração do código da máquina Enigma, evitou-se a morte de milhares de pessoas, e que tal feito pode ter contribuído, também, para ter abreviado a duração da Segunda Guerra. Reside nesse feito a importância indubitável do invento de Alan Turing, a bomba criptográfica capaz de decifrar qualquer cifra da máquina Enigma.

Turing também foi imortalizado por sua maior contribuição para a máquina que possibilitou a Era da Informação. Cerca de 20 anos depois de sua morte, dois estudantes universitários de 19 anos, que trabalhavam na garagem de seus pais, montaram o primeiro computador doméstico completo. A máquina, bem como sua nova empresa,

foi chamada de *Apple* (VOLKMAN, 2013). Apenas algumas pessoas compreenderam o significado do logotipo da empresa: uma maçã com uma única mordida.

Para além das questões históricas e computacionais tratadas no decorrer do projeto integrador, também tivemos o cuidado de, após a execução do mesmo, fazer uma avaliação sobre os ganhos educacionais e cognitivos propiciados no transcorrer desse itinerário educativo. O primeiro aspecto digno de realce foi o fato de que o projeto promoveu, de forma efetiva, a integração entre componentes curriculares da área profissional (Segurança em Redes de Computadores, Tópicos Especiais, Redes de Computadores III) e da base nacional comum (História, Sociologia e Filosofia), portanto, a proposta subsumida à realização de um projeto integrador não ficou “somente no papel”, houve uma integração efetiva de conteúdos das disciplinas que compõem o curso de educação profissional integrada ao Ensino Médio em questão. A partir da exposição dos seminários, percebemos, também, que as aulas e discussões promovidas propiciaram aos alunos a compreensão acerca da importância da criptografia como mecanismo eficaz para a transmissão de mensagens secretas, tanto em nível de comunicação entre Estados, quanto entre pessoas. Constatamos, também, que os(as) alunos(as) compreenderam como Alan Turing e suas invenções/ inovações foram fundamentais para o desenvolvimento da moderna computação. Verificamos ainda, por meios dos seminários, que houve entendimento abrangente acerca da importância da criptografia para o sigilo das informações em redes de computadores e em banco de dados.

Outro aspecto importante de ser destacado foi a proficuidade, do ponto de vista educacional, de se ter promovido maior interação, intercâmbio de conhecimentos e troca de práticas metodológicas entre os professores envolvidos no projeto integrador, sobretudo a partir da experiência da docência compartilhada. Além disso, verificamos maior interação, também, entre os(as) alunos(as) da turma, tendo em vista que o critério de formação dos grupos dos seminários levou em conta o fato de os(as) integrantes não terem muita afinidade entre eles, o que foi um dado positivo, pois estudantes que, geralmente, não se reuniam em grupos em ocasiões anteriores acabaram constituindo equipes para a realização desses seminários. Outro ganho importante a se destacar foi o fato de que as notas relativas à participação dos alunos no projeto se deu através de um processo democrático de avaliação das atividades desenvolvidas por eles/elas, pois os(as) próprios(as) estudantes fizeram uma autoavaliação de seus trabalhos que, somada à avaliação feita pelos docentes, foi constituída uma média final do projeto integrador. Ao final, viabilizamos também a oitiva dos(as) alunos(as) em relação às atividades desenvolvidas durante o projeto, o que também foi um ponto muito positivo, pois foi possível ter a dimensão do entendimento que os(as) estudantes que tiveram da proposta de integração curricular.

REFERÊNCIAS

- BRASIL. **Lei Federal nº 9394**, de 20 de dezembro de 1996. Brasília: Presidência da República, Casa Civil.
- BRASIL. **Decreto nº 5.154**, de 23 de julho de 2004. Brasília: Presidência da República, Casa Civil.
- BRASIL. **Lei Federal nº 11.741**, de 16 de julho de 2008. Brasília: Presidência da República, Casa Civil.
- BRASIL. **Lei Federal nº 11.892**, de 29 de dezembro de 2008. Brasília: Presidência da República, Casa Civil.
- CIAVATTA, M. A formação integrada: a escola e o trabalho como lugares de memória e de identidade. **Revista Trabalho Necessário**, Rio de Janeiro, vol. 3, n. 3, p. 1-20, 2005.
- HOBSBAWN, Eric. **A Era dos extremos: o breve século XX**. Trad. Marcos Santarrita. São Paulo: Cia das Letras, 1995.
- LEAVITT, D. **O homem que sabia demais: Alan Turing e a invenção do computador**. Trad. Samuel Dirceu. Ribeirão Preto/SP: Novo Conceito Editora, 2011.
- MARRA, Georges M. **O Jogo da Mimese e o Uso da Criptografia**. Dissertação de Mestrado. Goiânia. Programa de Mestrado em História da Pontifícia Universidade Católica de Goiás PUC Goiás, 2017, 216 p.
- MASSON, P. **A Segunda Guerra Mundial - História e Estratégias**. Trad. Ângela M. S. Corrêa. São Paulo: Editora Contexto, 2015.
- MATO, Omar L. **Ciencia y mitos en la Alemania de Hitler**. Ciudad Autonoma de Buenos Aires: Javier Vergara Editor, 2016
- O JOGO da imitação (The Imitation Game). Direção: Morten Tyldum. Produção: Nora Grossman, Ido Ostrowsky, Teddy Schwarzman. Intérpretes: Benedict Cumberbatch, Keira Knightley, Matthew Goode. Roteiro: Graham Moore. Reino Unido/Estados Unidos. Distribuição: Studio Canal (Reino Unido), The Weinstein Company (Estados Unidos), 2014, color., 114 min.
- SINGH, S. **O livro dos códigos**. Rio de Janeiro: Editora Record, 2014.
- TKOTZ, Viktoria. **Criptografia: segredos embalados para viagem**. São Paulo: Novatec Editora, 2005.
- VOLKMAN, E. **A História da Espionagem**. São Paulo: Editora Escala, 2013.
- ZOCHIO, M. **Introdução à Criptografia**. São Paulo: Novatec Editora, 2016.

SOBRE A ORGANIZADORA

DENISE PEREIRA Mestre em Ciências Sociais Aplicadas, Especialista em História, Arte e Cultura, Bacharel em História, pela Universidade Estadual de Ponta Grossa. Cursando Pós-Graduação Tecnologias Educacionais, Gestão da Comunicação e do Conhecimento. Atualmente Professora/Tutora Ensino a Distância da Universidade Estadual de Ponta Grossa (UEPG) e professora nas Faculdade Integradas dos Campos Gerais (CESCAGE) e Coordenadora de Pós-Graduação.

Agência Brasileira do ISBN
ISBN 978-85-7247-282-1

