**Introduzione**
L'idea che vorrei sottoporle è la seguente: un e-shop che vende capi in edizione limitata dotato di un sistema di difesa configurabile per monitorare e limitare il traffico automatizzato. Infatti, non si limiterebbe ad essere una semplice vetrina dei prodotti: il core dell'applicativo è sviluppare un sistema di difesa contro bot automatici, dai quali, un sito che vende items in tiratura limitata con elevata domanda, potrebbe essere oggetto di attacco.
Questo "antibot" ha dunque lo scopo di bloccare il traffico automatizzato attraverso varie tecniche, che verranno illustrate più nel dettaglio successivamente.
Lo shop è chiamato "Tie Dye", riprendendo la tecnica utilizzata per realizzare i capi che vengono venduti.

**Font e scelte stilistiche**
Il font utilizzato è "Inter", nelle variabili "Light", "Regular", "Medium".

*#D3EBFE* *#F7FBFF* *#F3F3F3* *#7689F5*

**Elenco delle pagine e funzioni utente**
Questi esempi di layout sono stati realizzati con Figma mentre il logo con Adobe Illustrator.

[AREA PUBBLICA]
Splash page con animazione sul logo

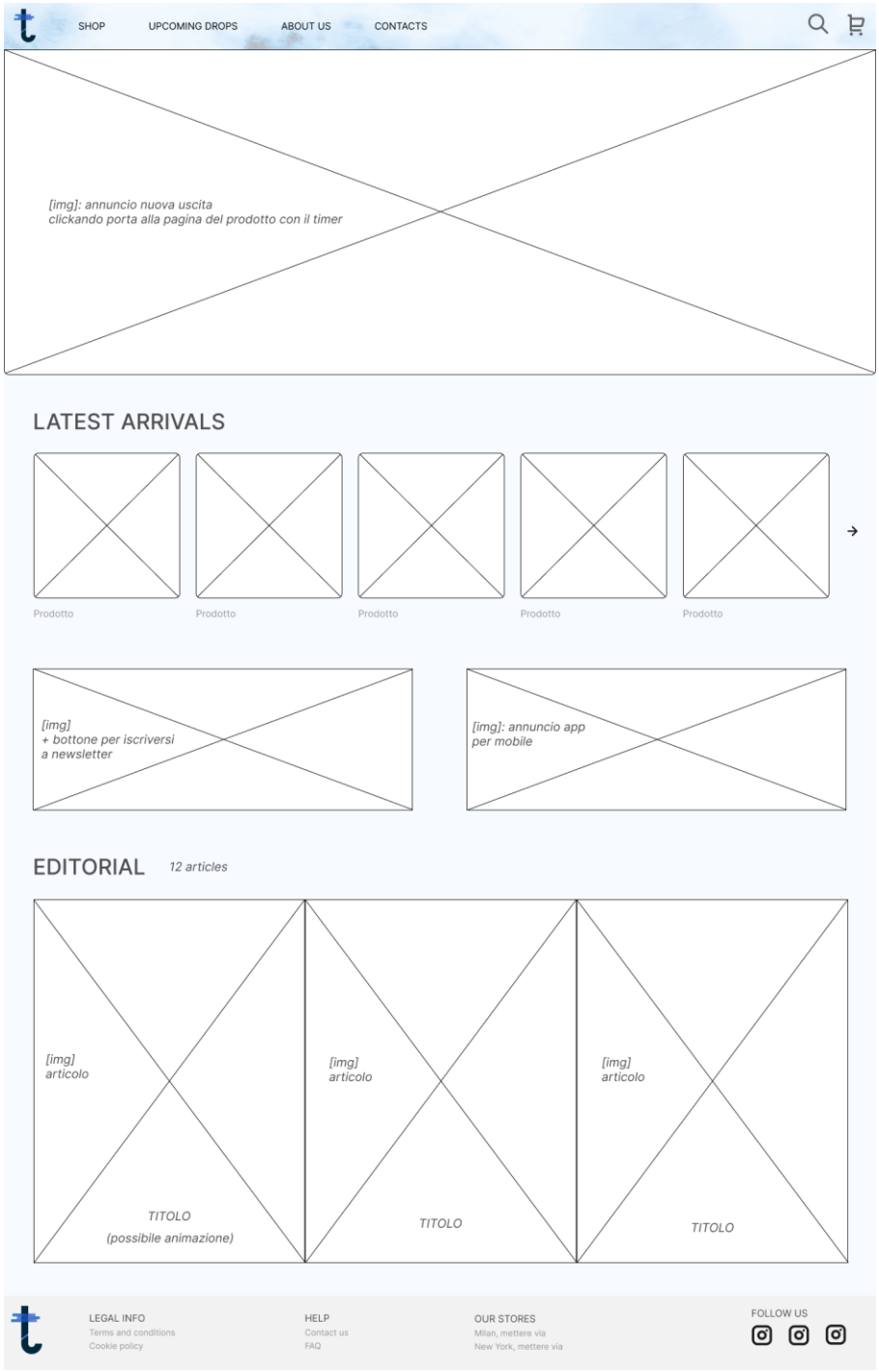




La splash page viene mostrata al caricamento del sito, la prima volta che si accede.
Potrebbe risultare utile per quando avvengono i primi check dell'antibot nel background, o anche come pagina di attesa per il sistema di coda. Ogni pagina dell'area pubblica contiene:

- Header: per navigare fra tutte le pagine, accedere al carrello o cercare direttamente prodotti nel catalogo
- Footer: "Contact us" è un'ancora al form presente nella pagina dei contatti. "Terms and conditions" apre un file PDF in una nuova finestra.

Home

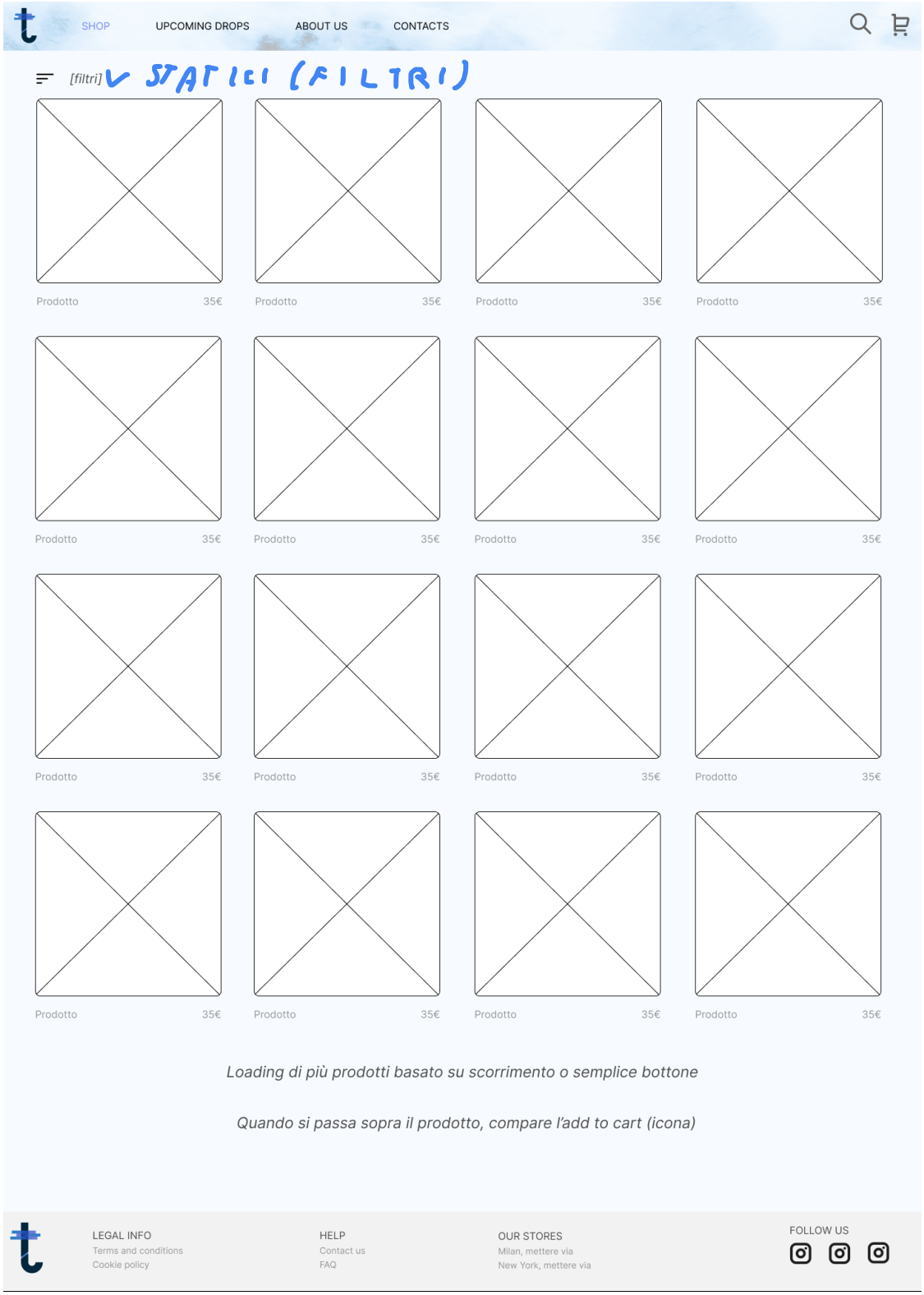



La home page è il punto di ingresso e contiene:

- Hero section per promuovere la prossima uscita
- La sezione “LATEST ARRIVALS” contiene dei prodotti cliccabili, che riportano alla pagina del prodotto. I prodotti sono inseriti dinamicamente dopo essere stati recuperati dal server. L’utente può scorrere i prodotti orizzontalmente.
- Banner di iscrizione alla newsletter + banner promozionale per l’app del sito
- Sezione “EDITORIAL”: alcune anteprime di articoli

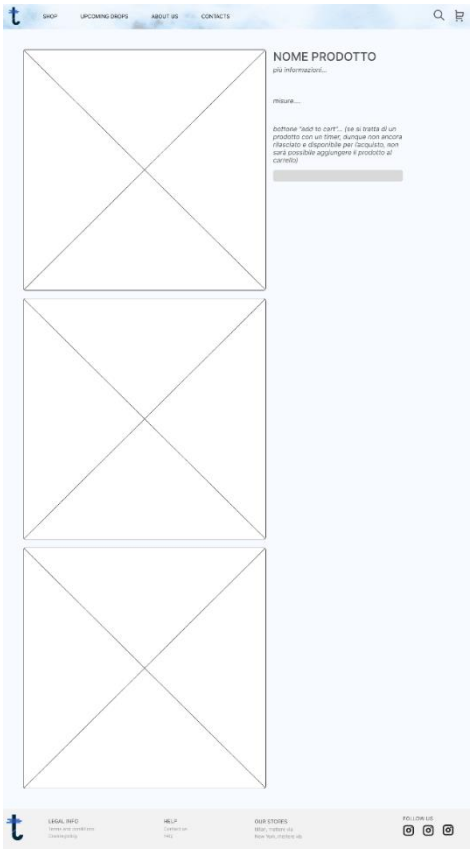
DINAMICA

Shop




- Filtri per restringere i prodotti visualizzati in base a caratteristiche come il prezzo.
- Una griglia con prodotti caricati dinamicamente. Arrivati in fondo, più prodotti (se presenti) potranno essere caricati cliccando un bottone (per non caricarli tutto allo stesso momento)
- Passando sopra un prodotto con il mouse, comparirà l'icona per aggiunge il prodotto al carrello

Pagina di un prodotto





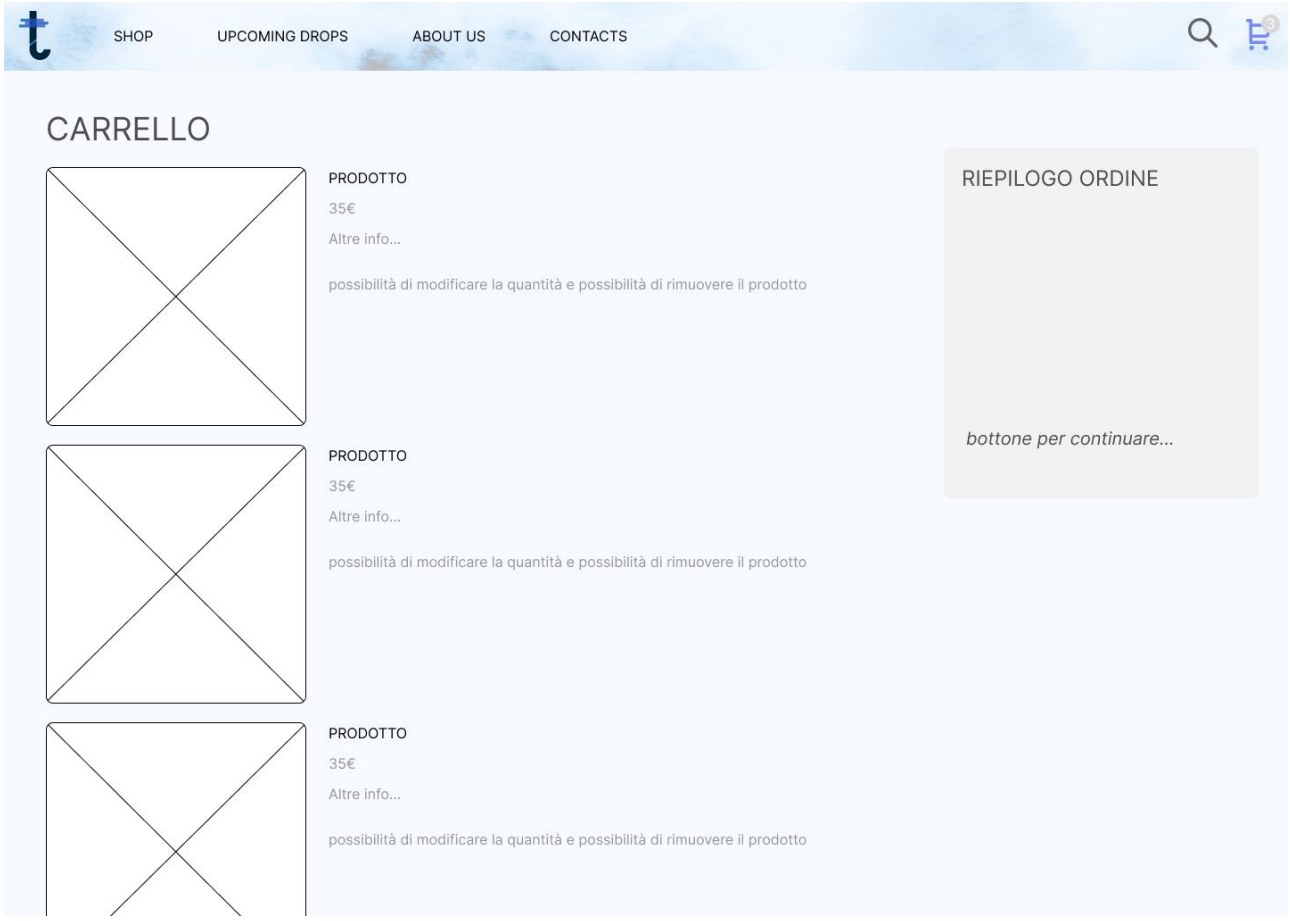


Ogni prodotto ha la propria pagina dedicata.
Passando sopra l'immagine con il mouse, avverrà uno zoom.
In questa pagina, l'utente potrà aggiungere il prodotto al carrello. L'endpoint verso il quale avverrà questa request è uno dei più sensibili, quindi sarà oggetto di rate limit. Superare il rate limit porterà a ricevere uno status *429 Too many Requests* sulle richieste successive, impedendo l'aggiunta di nuovi articoli.
Se il prodotto è aggiunto al carrello con successo, viene aperta una barra laterale a destra per potere procedere.
Un prodotto non ancora uscito avrà un timer, e non sarà possibile aggiungerlo al carrello.



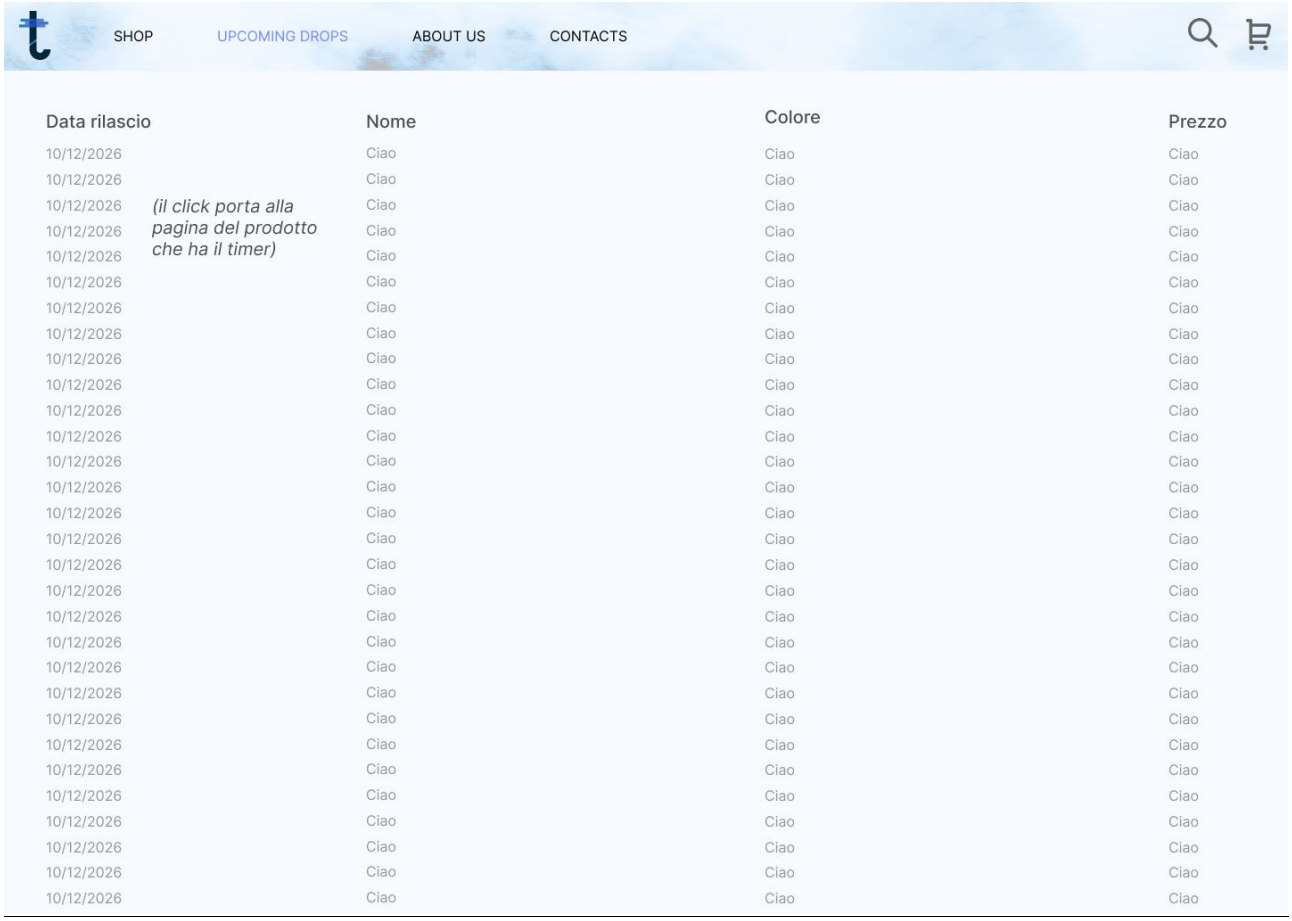
DINAMICA

Carrello




- Per ogni prodotto aggiunto al carrello viene mostrata l'immagine, il nome, il prezzo ed altre eventuali informazioni
- Sarà possibile modificare la quantità per ogni articolo o anche rimuovere l'articolo dal carrello
- A destra, una sezione che riepiloga l'ordine, con informazioni come il numero totale degli articoli, il totale del prezzo.
- Bottone per procedere (non porterà da nessuna parte)
- Per salvare il carrello viene utilizzato un cookie: questo contiene un identificatore del carrello. Nel database, l'identificatore viene associato ai prodotti inseriti

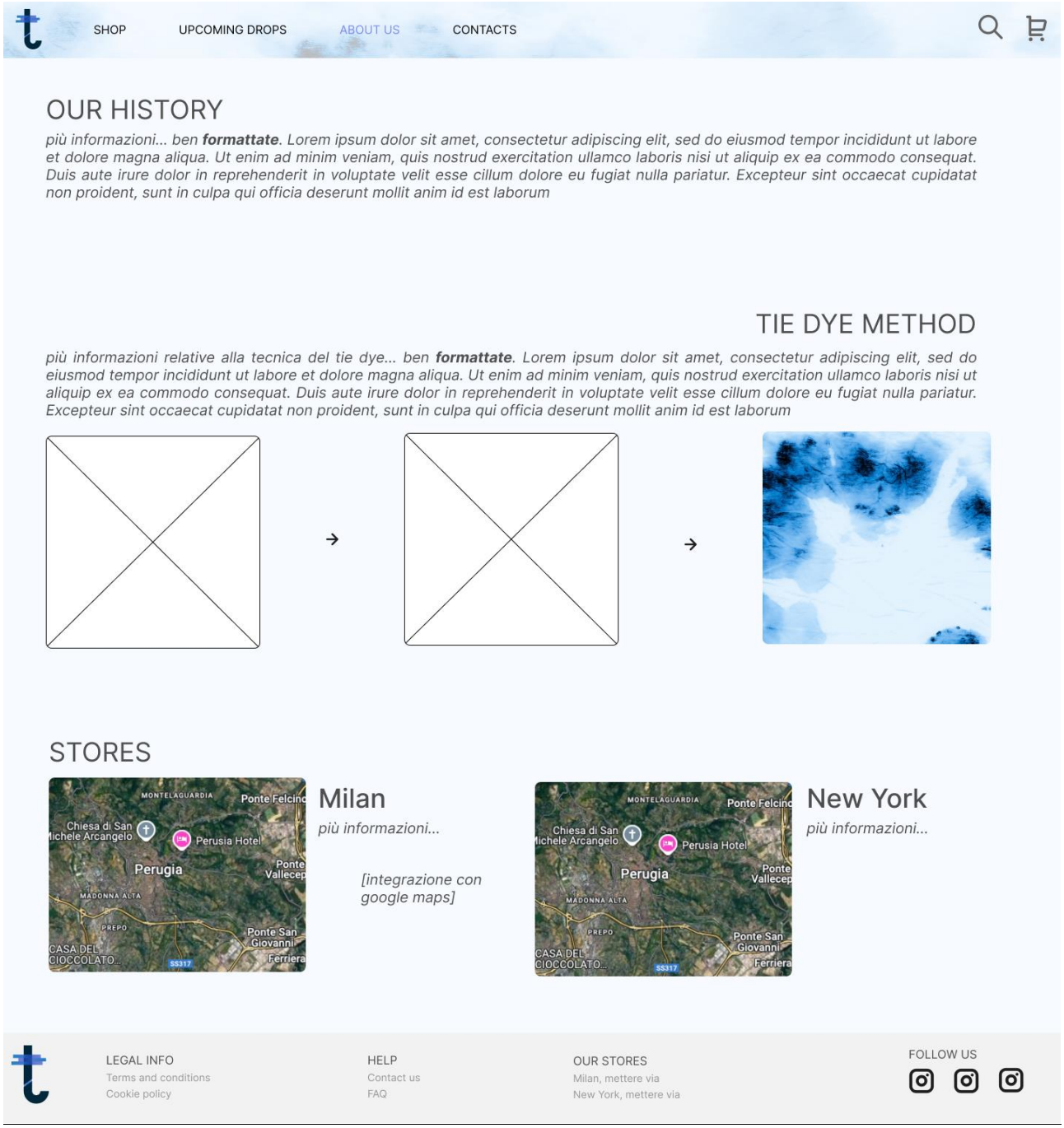
Upcoming drops DINAMICA




- Tabella delle prossime uscite

About us

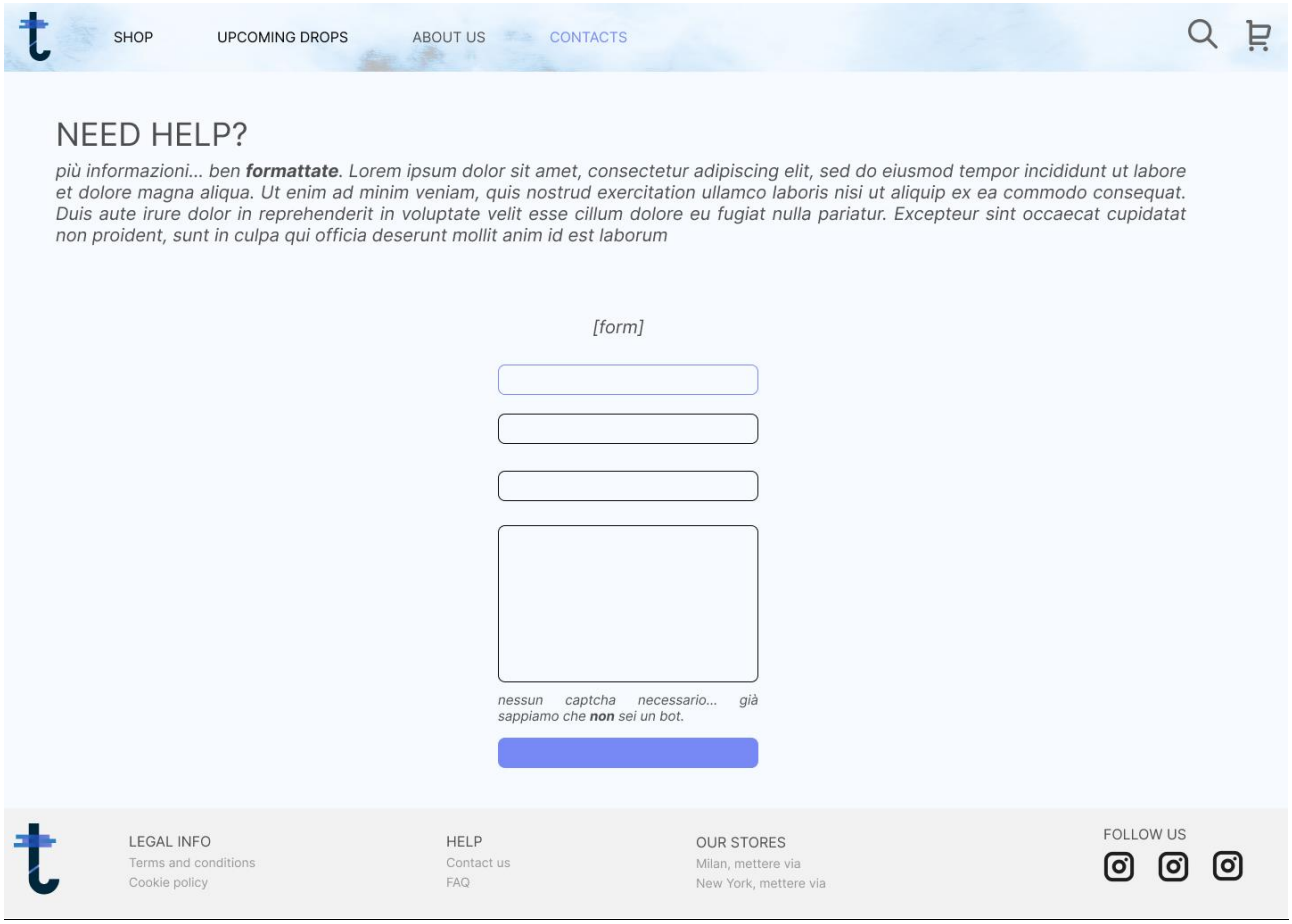
STATICA




- Sezione “OUR HISTORY” con qualche informazione sulla storia dello shop
- Sezione “TIE DYE METHOD” che descrive e illustra qualche passaggio della tecnica tie-dye, utilizzata per creare i capi
- Sezione “STORES”, con mappa interattiva Google Maps

STATICA

Contacts

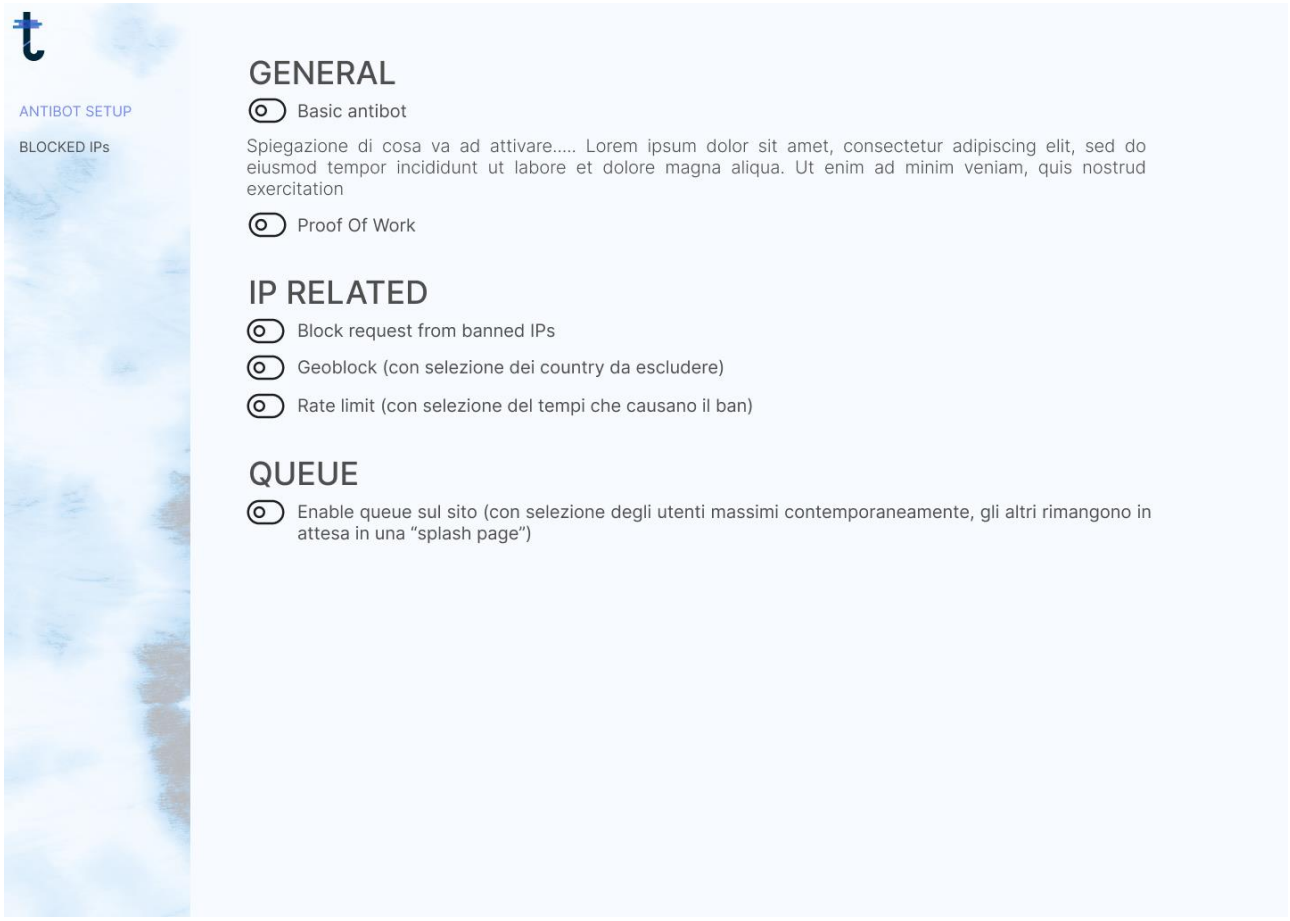



- Sezione “NEED HELP?” che spiega brevemente i motivi per cui puoi contattare il supporto.
- Form di contatto dove vengono chieste informazioni obbligatorie come il nome, l’indirizzo mail, l’oggetto e il messaggio. Segue il bottone per l’invio.

[AREA AMMINISTRATORE]

Queste due pagine sono private e accessibili solo per l'amministratore. L'autenticazione sarà gestita tramite JWT.
Il menù laterale permette di navigare fra le pagine.

Antibot setup




La pagina "ANTIBOT SETUP" permette di configurare il sistema di antibot attivo nel sito.

- Sezione "GENERAL"
- Sezione "IP RELATED"
- Sezione "QUEUE"

Blocked IPs




Questa pagina è formata da:

- Sezione “Statistics”: presenta un Google Chart per visualizzare il numero di IP bloccati per Location o per ASN, da decidere. (esempio: 10 IP geolocalizzati in Italia sono stati bloccati)
- Tabella degli indirizzi IP bloccati (recuperati dinamicamente), con possibilità di essere sbloccato.

**Struttura dell'antibot**

Cookie come "token" di accesso antibot
Il server genera un token solo dopo aver verificato che il client abbia superato tutti i controlli. Questo token (firmato dal server) contiene campi come l'identificatore, data di emissione, la data di scadenza, livello di autorizzazione. Ad ogni operazione sensibile, il token viene controllato dal server.

Dunque, ottenere il cookie equivale a superare tutti i controlli. Alcuni esempi di controlli che mi piacerebbe implementare sono elencati di seguito. Premetto che un bot evoluto sarà sempre in grado di superarli e mimare perfettamente un utente reale, il mio scopo non è raggiungere livelli di protezione come quelli offerti da Akamai, Cloudflare, Data Dome, etc... ma solo quello di utilizzare certi strumenti.

Possibili controlli iniziali:

1. L'IP address del client non deve essere bloccato.
2. presenza ed esecuzione di JavaScript;
3. presenza di window, document e navigator;
4. soluzione di un piccolo calcolo eseguito nel browser (una specie di proof-of-work, magari tramite web worker. Non si tratterebbe di un calcolo pesanti per evitare troppi rallentamenti);
5. scrolling, movimenti del mouse, clicks...

Blocco dell'IP
Come detto, un IP non deve essere bloccato per poter ottenere il cookie.
Un IP può diventare bloccato in base a determinati fattori:

- superamento del rate limit dovuto al numero di richieste che effettua (refresh della pagina, aggiunta al carrello... in generale sulla maggior parte degli endpoint esposti). In questo caso il server restituirà lo stato "429 Too Many Requests"
- IP non geolocalizzato in determinati paesi. L'amministratore può decidere quali regioni del mondo far accedere. Chiaramente, sarà necessario utilizzare strumenti di terze parti come ipinfo.io per ottenere queste informazioni.
- IP appartenente a certe subnet o ASN.

La lista degli IP bloccati viene archiviata nel database ed è gestibile tramite la dashboard dell'amministratore, che può sbloccare i singoli IP.

Sarò in grado di presentare i vari casi di blocco, anche tramite request che utilizzano proxies geolocalizzati in molte regioni del globo. Questo potrebbe implicare di dover rendere il server pubblico o utilizzare altri metodi per dimostrare l'efficacia del sistema.

Sistema di coda
Durante i rilasci di prodotti con alta domanda, è spesso utile impostare un numero massimo di utenti contemporanei presenti nel sito.
Presumo di fare un polling con fetch per interrogare lo stato della coda e verificare se l'utente può accedere al sito (questo avverrà comunque dopo aver superato l'antibot).

**Database**

Il database archivia informazioni sia per la parte pubblica che per la parte amministrativa.
Per la parte pubblica vengono memorizzate informazioni relative a:

- catalogo (prodotti e informazioni relative ad essi, come il prezzo, la quantità disponibile)
- lista degli “upcoming drops” (con il prodotto in uscita, la data di rilascio)
- prodotti presenti nei carrelli, con variante e quantità inserita (associati tramite il cookie)

Per la parte amministrativa:

- Credenziali amministratore
- Configurazione del sistema antibot
- IP bloccati
- Eventuali ticket della coda